NSX Administration Guide

NSX 6.1 for vSphere

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001543-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

NSX Administration Guide 11

1 Overview of NSX 13
- NSX Components 14
- NSX Services 16

2 Logical Switches 19
- Create a Logical Switch 20
- Connect Virtual Machines to a Logical Switch 23
- Test Logical Switch Connectivity 23
- Prevent Spoofing on a Logical Switch 24
- Edit a Logical Switch 24
- Working with Transport Zones 24
- Logical Switch Scenario 26

3 L2 Bridges 31
- Add L2 Bridge 32

4 Logical Router 33
- Specify Global Configuration 33
- Add a Static Route 34
- Configure OSPF 35
- Configure BGP 36
- Configure IS-IS Protocol 37
- Configure Route Redistribution 38

5 Logical Firewall 41
- Distributed Firewall 41
- Edge Firewall 42
- Working with Firewall Rules 42
- Working with Firewall Rule Sections 50
- Working with Firewall Configurations 51
- Excluding Virtual Machines from Firewall Protection 52
- Using SpoofGuard 53
- View Firewall CPU and Memory Threshold Events 56
- Firewall Logs 56
- Working with Local Rules 56

6 Virtual Private Networks (VPN)s 65
- SSL VPN-Plus Overview 65
- IPSec VPN Overview 85

L2 VPN Overview 89

7 Logical Load Balancer 97
Set Up Load Balancing 97
Working with Application Profiles 105
Working with Service Monitors 105
Working with Server Pools 106
Working with Virtual Servers 106
Working with Application Rules 107

8 Other Edge Services 109
Managing DHCP Service 109
Configuring DHCP Relay 112
Configure DNS Servers 113

9 Service Composer 115
Using Service Composer 116
Graphical View of Service Composer 122
Export a Service Composer Configuration 125
Import a Service Composer Configuration 125
Working with Security Tags 126
Viewing Effective Services 127
Working with Security Policies 129
Edit a Security Group 130
Service Composer Scenarios 130

10 Data Security 135
NSX Data Security User Roles 135
Defining a Data Security Policy 135
Running a Data Security Scan 137
Viewing and Downloading Reports 138
Creating Regular Expressions 138

11 Network Extensibility 139
Distributed Service Insertion 140
Edge-Based Service Insertion 140
Integrating Third Party Services 140
Consuming Vendor Services through Service Composer 140
Redirecting Traffic to a Vendor Solution through Logical Firewall 141
Using a Partner Load Balancer 141

12 User Management 143
Configure Single Sign On 143
Managing User Rights 144
Managing the Default User Account 145
Assign a Role to a vCenter User 145
Edit a User Account 147
Change a User Role 148

Disable or Enable a User Account 148
Delete a User Account 148

13 Network and Security Objects 149
Working with IP Address Groups 149
Working with MAC Address Groups 150
Working with IP Pools 151
Working with Security Groups 152
Working with Services and Service Groups 154

14 Operations and Management 157
System Events and Audit Logs 157
Management System Settings 161
Working with Active Directory Domains 164
NSX Edge Operations 166
Backing Up NSX Manager Data 178
Flow Monitoring 179
Activity Monitoring 186
Guest Introspection Events and Alarms 195

15 NSX Edge VPN Configuration Examples 199
Terminology 200
IKE Phase 1 and Phase 2 200
Configuring IPSec VPN Service Example 202
Using a Cisco 2821 Integrated Services Router 203
Using a Cisco ASA 5510 206
Configuring a WatchGuard Firebox X500 208
Troubleshooting NSX Edge Configuration Example 209

16 Data Security Regulations 219
Arizona SB-1338 221
ABA Routing Numbers 221
Australia Bank Account Numbers 221
Australia Business and Company Numbers 221
Australia Medicare Card Numbers 222
Australia Tax File Numbers 222
California AB-1298 222
California SB-1386 223
Canada Social Insurance Numbers 223
Canada Drivers License Numbers 223
Colorado HB-1119 224
Connecticut SB-650 224
Credit Card Numbers 224
Custom Account Numbers 224
EU Debit Card Numbers 225
FERPA (Family Educational Rights and Privacy Act) 225
Florida HB-481 225
France IBAN Numbers 225

France National Identification Numbers Policy 225
Georgia SB-230 Policy 226
Germany BIC Numbers Policy 226
Germany Driving License Numbers Policy 226
Germany IBAN Numbers Policy 226
Germany National Identification Numbers Policy 226
Germany VAT Numbers Policy 226
Hawaii SB-2290 Policy 227
HIPAA (Healthcare Insurance Portability and Accountability Act) Policy 227
Idaho SB-1374 Policy 227
Illinois SB-1633 228
Indiana HB-1101 Policy 228
Italy Driving License Numbers Policy 228
Italy IBAN Numbers Policy. 228
Italy National Identification Numbers Policy 228
Kansas SB-196 Policy 229
Louisiana SB-205 Policy 229
Maine LD-1671 Policy 229
Massachusetts CMR-201 230
Minnesota HF-2121 230
Montana HB-732 230
Netherlands Driving Licence Numbers 230
Nevada SB-347 231
New Hampshire HB-1660 231
New Jersey A-4001 231
New York AB-4254 232
New Zealand Inland Revenue Department Numbers 232
New Zealand Ministry of Health Numbers 232
Ohio HB-104 232
Oklahoma HB-2357 233
Patient Identification Numbers 233
Payment Card Industry Data Security Standard (PCI-DSS) 233
Texas SB-122 233
UK BIC Numbers 234
UK Driving Licence Numbers 234
UK IBAN Numbers 234
UK National Health Service Numbers 234
UK National Insurance Numbers (NINO) 234
UK Passport Numbers 234
US Drivers License Numbers 235
US Social Security Numbers 235
Utah SB-69 235
Vermont SB-284 235
Washington SB-6043 236
Data Security Content Blades 236

17 Data Security Content Blades 257
ABA Routing Number Content Blade 260
Admittance and Discharge Dates Content Blade 260

Alabama Drivers License Content Blade 260
Alaska Drivers License Content Blade 261
Alberta Drivers Licence Content Blade 261
Alaska Drivers License Content Blade 261
Alberta Drivers Licence Content Blade 261
American Express Content Blade 261
Arizona Drivers License Content Blade 261
Arkansas Drivers License Content Blade 262
Australia Bank Account Number Content Blade 262
Australia Business Number Content Blade 262
Australia Company Number Content Blade 262
Australia Medicare Card Number Content Blade 262
Australia Tax File Number Content Blade 262
California Drivers License Number Content Blade 263
Canada Drivers License Number Content Blade 263
Canada Social Insurance Number Content Blade 263
Colorado Drivers License Number Content Blade 263
Connecticut Drivers License Number Content Blade 263
Credit Card Number Content Blade 263
Credit Card Track Data Content Blade 263
Custom Account Number Content Blade 264
Delaware Drivers License Number Content Blade 264
EU Debit Card Number Content Blade 264
Florida Drivers License Number Content Blade 264
France Driving License Number Content Blade 264
France BIC Number Content Blade 264
France IBAN Number Content Blade 264
France National Identification Number Content Blade 265
France VAT Number Content Blade 265
Georgia Drivers License Number Content Blade 265
Germany BIC Number Content Blade 265
Germany Driving License Number Content Blade 265
Germany IBAN Number Content Blade 265
Germany National Identification Numbers Content Blade 265
Germany Passport Number Content Blade 266
Germany VAT Number Content Blade 266
Group Insurance Numbers Content Blade 266
Hawaii Drivers License Number Content Blade 266
Italy National Identification Numbers Content Blade 266
Health Plan Beneficiary Numbers 267
Idaho Drivers License Number Content Blade 267
Illinois Drivers License Number Content Blade 267
Indiana Drivers License Number Content Blade 267
Iowa Drivers License Number Content Blade 267
Index of Procedures Content Blade 267
Italy Driving License Number Content Blade 268
Italy IBAN Number Content Blade 268
ITIN Unformatted Content Blade 268
Kansas Drivers License Number Content Blade 269

Kentucky Drivers License Number Content Blade 269
Louisiana Drivers License Number Content Blade 269
Maine Drivers License Number Content Blade 269
Manitoba Drivers Licence Content Blade 269
Maryland Drivers License Number Content Blade 270
Massachusetts Drivers License Number Content Blade 270
Michigan Drivers License Number Content Blade 270
Minnesota Drivers License Number Content Blade 270
Mississippi Drivers License Number Content Blade 270
Missouri Drivers License Number Content Blade 270
Montana Drivers License Number Content Blade 270
NDC Formulas Dictionary Content Blade 270
Nebraska Drivers License Number Content Blade 271
Netherlands Driving Licence Number Content Blade 271
Netherlands IBAN Number Content Blade 271
Netherlands National Identification Numbers Content Blade 271
Netherlands Passport Number Content Blade 272
Nevada Drivers License Number Content Blade 272
New Brunswick Drivers Licence Content Blade 272
New Hampshire Drivers License Number Content Blade 272
New Jersey Drivers License Number Content Blade 272
New Mexico Drivers License Number Content Blade 272
New York Drivers License Number Content Blade 272
New Zealand Health Practitioner Index Number Content Blade 273
New Zealand Inland Revenue Department Number 273
New Zealand National Health Index Number Content Blade 273
Newfoundland and Labrador Drivers Licence Content Blade 273
North Carolina Drivers License Number Content Blade 273
North Dakota Drivers License Number Content Blade 273
Nova Scotia Drivers Licence Content Blade 273
Ohio Drivers License Number Content Blade 273
Oklahoma License Number Content Blade 274
Ontario Drivers Licence Content Blade 274
Oregon License Number Content Blade 274
Patient Identification Numbers Content Blade 274
Pennsylvania License Number Content Blade 274
Prince Edward Island Drivers Licence Content Blade 274
Protected Health Information Terms Content Blade 274
Quebec Drivers Licence Content Blade 275
Rhode Island License Number Content Blade 275
Saskatchewan Drivers Licence Content Blade 275
SIN Formatted Content Blade 275
SIN Unformatted Content Blade 275
SSN Formatted Content Blade 275
SSN Unformatted Content Blade 276
South Carolina License Number Content Blade 276
South Dakota License Number Content Blade 276
Spain National Identification Number Content Blade 276
Spain Passport Number Content Blade 276

Spain Social Security Number Content Blade 276
Sweden IBAN Number Content Blade 276
Sweden Passport Number Content Blade 277
Tennessee License Number Content Blade 277
UK BIC Number Content Blade 277
UK Driving License Number Content Blade 277
UK IBAN Number Content Blade 278
UK National Health Service Number Content Blade 278
UK NINO Formal Content Blade 278
UK Passport Number Content Blade 278
Utah License Number Content Blade 279
Virginia License Number Content Blade 279
Visa Card Number Content Blade 279
Washington License Number Content Blade 279
Wisconsin License Number Content Blade 279
Wyoming License Number Content Blade 279

18 File Formats Supported by Data Security 281

Index 287

NSX Administration Guide

The *NSX Administration Guide* describes how to configure, monitor, and maintain the VMware® NSX™ system by using the NSX Manager user interface and the vSphere Web Client. The information includes step-by-step configuration instructions, and suggested best practices.

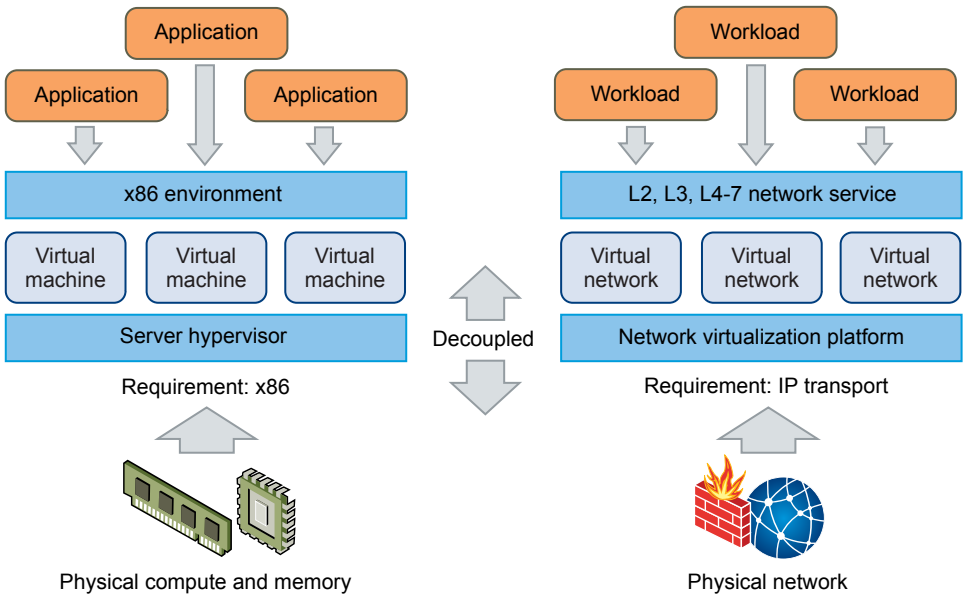
Intended Audience

This manual is intended for anyone who wants to install or use NSX in a VMware vCenter environment. The information in this manual is written for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This manual assumes familiarity with VMware Infrastructure 5.x, including VMware ESX, vCenter Server, and the vSphere Web Client.

1 Overview of NSX

IT organizations have gained significant benefits as a direct result of server virtualization. Server consolidation reduced physical complexity, increased operational efficiency and the ability to dynamically re-purpose underlying resources to quickly and optimally meet the needs of increasingly dynamic business applications.

VMware's Software Defined Data Center (SDDC) architecture is now extending virtualization technologies across the entire physical data center infrastructure. VMware NSX®, the network virtualization platform, is a key product in the SDDC architecture. With NSX, virtualization delivers for networking what it has already delivered for compute and storage. In much the same way that server virtualization programmatically creates, snapshots, deletes and restores software-based virtual machines (VMs), NSX network virtualization programmatically creates, snapshots, deletes, and restores software-based virtual networks. The result is a completely transformative approach to networking that not only enables data center managers to achieve orders of magnitude better agility and economics, but also allows for a vastly simplified operational model for the underlying physical network. With the ability to be deployed on any IP network, including both existing traditional networking models and next-generation fabric architectures from any vendor, NSX is a completely non-disruptive solution. In fact, with NSX, the physical network infrastructure you already have is all you need to deploy a software-defined data center.



The figure above draws an analogy between compute and network virtualization. With server virtualization, a software abstraction layer (server hypervisor) reproduces the familiar attributes of an x86 physical server (for example, CPU, RAM, Disk, NIC) in software, allowing them to be programmatically assembled in any arbitrary combination to produce a unique VM in a matter of seconds.

With network virtualization, the functional equivalent of a network hypervisor reproduces the complete set of Layer 2 through Layer 7 networking services (for example, switching, routing, access control, firewalling, QoS, and load balancing) in software. As a result, these services can be programmatically assembled in any arbitrary combination, to produce unique, isolated virtual networks in a matter of seconds.

With network virtualization, benefits similar to server virtualization are derived. For example, just as VMs are independent of the underlying x86 platform and allow IT to treat physical hosts as a pool of compute capacity, virtual networks are independent of the underlying IP network hardware and allow IT to treat the physical network as a pool of transport capacity that can be consumed and repurposed on demand. Unlike legacy architectures, virtual networks can be provisioned, changed, stored, deleted, and restored programmatically without reconfiguring the underlying physical hardware or topology. By matching the capabilities and benefits derived from familiar server and storage virtualization solutions, this transformative approach to networking unleashes the full potential of the software-defined data center.

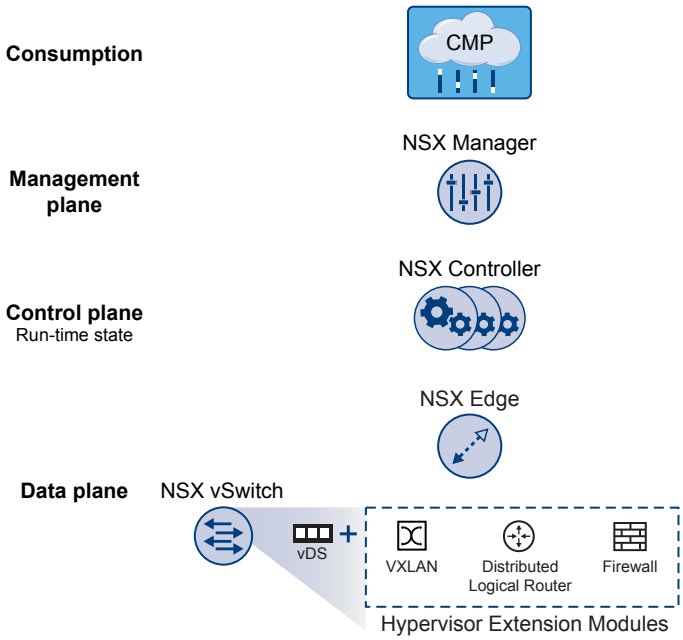
NSX can be configured through the vSphere Web Client, a command-line interface (CLI), and a REST API.

This chapter includes the following topics:

- "NSX Components," on page 14
- "NSX Services," on page 16

NSX Components

This section describes the components of the NSX solution.



Data Plane

The NSX Data plane consists of the NSX vSwitch, which is based on the vSphere Distributed Switch (VDS) with additional components to enable services. Kernel modules (VIBs) run within the hypervisor kernel to provide services such as distributed routing and logical firewall and to enable VXLAN bridging capabilities.

The NSX vSwitch (vDS-based) abstracts the physical network and provides access-level switching in the hypervisor. It is central to network virtualization because it enables logical networks that are independent of physical constructs, such as VLANs. Some of the benefits of the vSwitch are:

- Support for overlay networking with protocols (such as VXLAN) and centralized network configuration. Overlay networking enables the following capabilities:
  - Creation of a flexible logical Layer 2 (L2) overlay over existing IP networks on existing physical infrastructure without the need to re-architect any of the data center networks
  - Provision of communication (east–west and north–south), while maintaining isolation between tenants
  - Application workloads and virtual machines that are agnostic of the overlay network and operate as if they were connected to a physical L2 network
- Facilitates massive scale of hypervisors
- Multiple features—such as Port Mirroring, NetFlow/IPFIX, Configuration Backup and Restore, Network Health Check, QoS, and LACP—provide a comprehensive toolkit for traffic management, monitoring, and troubleshooting within a virtual network

Additionally, the data plane consists of gateway devices that can provide L2 bridging from the logical networking space (VXLAN) to the physical network (VLAN). The gateway device is typically an NSX Edge virtual appliance. NSX Edge offers L2, L3, perimeter firewall, load balancing, and other services such as SSL VPN and DHCP.

Control Plane

The NSX control plane runs in the NSX controller. NSX controller is an advanced distributed state management system that controls virtual networks and overlay transport tunnels. It is the central control point for all logical switches within a network and maintains information about all virtual machines, hosts, logical switches, and VXLANs.

The controller does not have any dataplane traffic passing through it. Controller nodes are deployed in a cluster of odd-numbered members to enable high-availability and scale. Any failure of the controller nodes does not impact any data-plane traffic.

Management Plane

The NSX management plane is built by the NSX Manager, the centralized network management component of NSX. It provides the single point of configuration and REST API entry-points.

The NSX Manager is installed as a virtual appliance on any ESX™ host in your vCenter Server environment.

Consumption Platform

The consumption of NSX can be driven directly through the NSX Manager user interface. In a vSphere environment, this is available in the vSphere Web Client. Typically end users tie network virtualization to their cloud management platform for deploying applications. NSX provides rich integration into virtually any CMP through REST APIs. Out-of-the-box integration is also available through VMware vCloud Automation Center, vCloud Director, and OpenStack with the Neutron plug-in for NSX.

NSX Services

The NSX components work together to provide the following functional services.

Logical Switches

A cloud deployment or a virtual data center has a variety of applications across multiple tenants. These applications and tenants require isolation from each other for security, fault isolation, and non-overlapping IP addresses. The NSX logical switch creates logical broadcast domains or segments to which an application or tenant virtual machine can be logically wired. This allows for flexibility and speed of deployment while still providing all the characteristics of a physical network's broadcast domains (VLANs) without physical Layer 2 sprawl or spanning tree issues.

A logical switch is distributed and can span arbitrarily large compute clusters. This allows for virtual machine mobility (vMotion) within the data center without limitations of the physical Layer 2 (VLAN) boundary. The physical infrastructure is not constrained by MAC/FIB table limits, because the logical switch contains the broadcast domain in software.

Logical Routers

Dynamic routing provides the necessary forwarding information between Layer 2 broadcast domains, thereby allowing you to decrease the size of Layer 2 broadcast domains and improve network efficiency and scale. NSX extends this intelligence to where the workloads reside for East-West routing. This allows more direct VM-to-VM communication without the costly or timely need to extend hops. At the same time, NSX logical routers provide North-South connectivity, thereby enabling tenants to access public networks.

Logical Firewall

Logical Firewall provides security mechanisms for dynamic virtual data centers. The Distributed Firewall component of Logical Firewall allows you to segment virtual datacenter entities like virtual machines based on VM names and attributes, user identity, vCenter objects like datacenters, and hosts, as well as traditional networking attributes like IP addresses, VLANs, and so on. The Edge Firewall component helps you meet key perimeter security requirements, such as building DMZs based on IP/VLAN constructs, tenant-to-tenant isolation in multi-tenant virtual data centers, Network Address Translation (NAT), partner (extranet) VPNs, and user-based SSL VPNs.

The Flow Monitoring feature displays network activity between virtual machines at the application protocol level. You can use this information to audit network traffic, define and refine firewall policies, and identify threats to your network.

Logical Virtual Private Networks (VPN)s

SSL VPN-Plus allows remote users to access private corporate applications. IPSec VPN offers site-to-site connectivity between an NSX Edge instance and remote sites. L2 VPN allows you to extend your datacenter by allowing virtual machines to retain network connectivity across geographical boundaries.

Logical Load Balancer

The NSX Edge load balancer enables network traffic to follow multiple paths to a specific destination. It distributes incoming service requests evenly among multiple servers in such a way that the load distribution is transparent to users. Load balancing thus helps in achieving optimal resource utilization, maximizing throughput, minimizing response time, and avoiding overload. NSX Edge provides load balancing up to Layer 7.

Service Composer

Service Composer helps you provision and assign network and security services to applications in a virtual infrastructure. You map these services to a security group, and the services are applied to the virtual machines in the security group.

Data Security provides visibility into sensitive data stored within your organization's virtualized and cloud environments. Based on the violations reported by NSX Data Security, you can ensure that sensitive data is adequately protected and assess compliance with regulations around the world.

NSX Extensibility

VMware partners can integrate their solutions with the NSX platform, thus enabling customers to have an integrated experience across VMware products and partner solutions. Data center operators can provision complex, multi-tier virtual networks in seconds, independent of the underlying network topology or components.

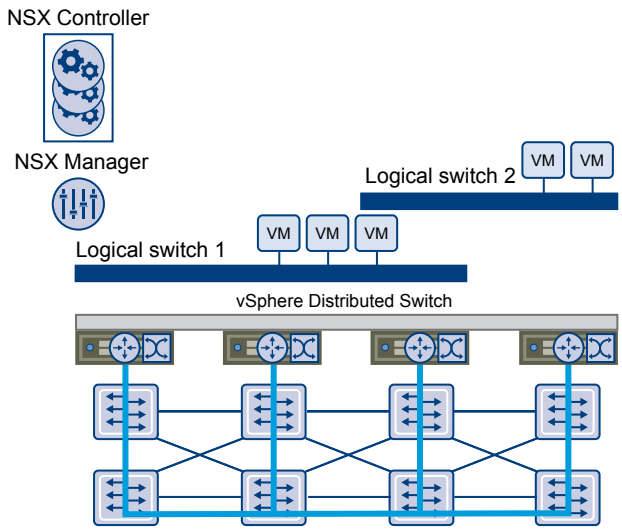
Logical Switches

2

A cloud deployment or a virtual data center has a variety of applications across multiple tenants. These applications and tenants require isolation from each other for security, fault isolation, and avoidance of overlapping IP addressing issues. The NSX logical switch creates logical broadcast domains or segments to which an application or tenant virtual machine can be logically wired. This allows for flexibility and speed of deployment while still providing all the characteristics of a physical network's broadcast domains (VLANs) without physical Layer 2 sprawl or spanning tree issues.

A logical switch is distributed and can span arbitrarily large compute clusters. This allows for virtual machine mobility (vMotion) within the datacenter without the limitations of the physical Layer 2 (VLAN) boundary. The physical infrastructure is not constrained by MAC/FIB table limits because the logical switch contains the broadcast domain in software.

A logical switch is mapped to a unique VXLAN, which encapsulates the virtual machine traffic and carries it over the physical IP network.



The NSX controller is the central control point for all logical switches within a network and maintains information aboutall virtual machines, hosts, logical switches, and VXLANs. The controller supports two new logical switch control plane modes, Unicast and Hybrid. These modes decouple NSX from the physical network. VXLANs no longer require the physical network to support multicast in order to handle the Broadcast, Unknown unicast, and Multicast (BUM) traffic within a logical switch. The unicast mode replicates all the BUM traffic locally on the host and requires no physical network configuration. In the hybrid mode, some of the BUM traffic replication is offloaded to the first hop physical switch to achieve better performance. This mode requires IGMP snooping to be enabled the first hop physical switch. Virtual machines within a logical switch can use and send any type of traffic including IPv6 and multicast.

You can extend a logical switch to a physical device by adding an L2 bridge. See Chapter 3, "L2 Bridges," on page 31.

You must have the Super Administrator or Enterprise Administrator role permissions to manage logical switches.

This chapter includes the following topics:

- "Create a Logical Switch," on page 20
- "Connect Virtual Machines to a Logical Switch," on page 23
- "Test Logical Switch Connectivity," on page 23
- "Prevent Spoofing on a Logical Switch," on page 24
- "Edit a Logical Switch," on page 24
- "Working with Transport Zones," on page 24
- "Logical Switch Scenario," on page 26

Create a Logical Switch

Prerequisites

- You have the Super Administrator or Enterprise Administrator role permission to configure and manage logical switches.
- You have prepared clusters that are to be part of the logical switch. See *Prepare Clusters for Network Virtualization* in the *NSX Installation and Upgrade Guide*.
- You have configured VXLAN on the appropriate clusters. See *Configure VXLAN Transport Parameters* in the *NSX Installation and Upgrade Guide*.
- You have the minimum required software versions. See *System Requirements* in the *NSX Installation and Upgrade Guide*.
- VXLAN UDP port is opened on firewall rules (if applicable). The VXLAN UDP port can be configured through the API. The default is 8472.
- Port 80 is opened from NSX Manager to the hosts. This is used to download the vib/agent.
- Physical infrastructure MTU is at least 50 bytes more than the MTU of the virtual machine vNIC.
- Managed IP address is set for each vCenter Server in the vCenter Server Runtime Settings. See *vCenter Server and Host Management*.
- DHCP is available on VXLAN transport VLANs if you are using DHCP for IP assignment for VMKNics.
- A consistent distributed virtual switch type (vendor, and so on) and version is being used across a given transport zone. Inconsistent switch types can lead to undefined behavior in your logical switch.
- 5-tuple hash distribution is enabled for Link Aggregation Control Protocol (LACP).
- For multicast mode, multicast routing is enabled if VXLAN traffic is traversing routers. You have aquired a multicast address range from your network administrator.
- (Recommended) You have enabled IGMP snooping on the L2 switches to which VXLAN participating hosts are attached. If IGMP snooping is enabled on L2, IGMP querier must be enabled on the router or L3 switch with connectivity to multicast enabled networks.

Add a Transport Zone

A transport zone defines the span of a logical switch. It can span one or more vSphere clusters. An NSX environment can contain one or more transport zones based on your requirements.

If a vDS spans more than one cluster and the transport zone is based on one of these clusters, the logical switch associated with this transport zone can access virtual machines within all clusters spanned by the vDS. In other words, this transport zone will not be able to constrain the logical switch span to a single cluster.

If this logical switch is later connected to a distributed router, you must ensure that the router instances are created only in the cluster included in the transport zone to avoid any Layer 3 issues.

Procedure

1 In the vSphere Web Client, click **Networking & Security > Installation**.

2 Click **Logical Network Preparation** and then click **Transport Zones**.

3 Click the **New Transport Zone** icon.

4 In the New Transport Zone dialog box, type a name and description for the transport zone.

5 Depending on whether you have a controller node in your environment, or you want to use multicast addresses, select the control plane mode.

- **Multicast**: Multicast IP addresses in the physical network are used for the control plane. This mode is recommended only when you are upgrading from older VXLAN deployments. Requires PIM/IGMP in the physical network.
- **Unicast** : The control plane is handled by an NSX controller. All unicast traffic leverages headend replication. No multicast IP addresses or special network configuration is required.
- **Hybrid** : The optimized unicast mode. Offloads local traffic replication to the physical network (L2 multicast). This requires IGMP snooping on the first-hop switch, but does not require PIM. The first-hop switch handles traffic replication for the subnet.

6 Select the clusters to be added to the transport zone.

7 Click **OK**.

Add a Logical Switch

A logical switch reproduces Layer 2 and Layer 3 switching functionality (unicast, multicast, broadcast) in a virtual environment completely decoupled from underlying hardware.

Procedure

1 In **Networking & Security**, click the **Logical Switches** tab.

2 Click the **New Logical Switch** icon.

3 Type a name and description for the logical switch.

4 Select the transport zone in which you want to create the virtualized network. The Scope Details panel displays the clusters that are part of the selected transport zone and the services available to be deployed on the scope.

5 By default, the logical switch inherits the control plane mode from the transport zone. You can change it to one of the other available modes:

- **Unicast**: The control plane is handled by an NSX controller. All traffic replication is handled locally by the hypervisor. No multicast IP addresses or special network configuration is required.
- **Hybrid**: The optimized unicast mode. Offloads local traffic replication to the physical network. This requires IGMP snooping on the first-hop switch, but does not require PIM. The first-hop switch handles traffic replication for the subnet.
- **Multicast**: Multicast IP addresses in the physical network are used for the control plane. This mode is recommended only when you are upgrading from older VXLAN deployments. Requires PIM/IGMP in the physical network.

6 Click **Enable IP Discovery** to enable ARP suppression.

7 Click **Enable MAC Learning** to avoid possible traffic loss during vMotion.

Enabling MAC Learning builds a VLAN/MAC pair learning table on each vNic. This table is stored as part of the dvfilter data. During vMotion, dvfilter saves and restores the table at the new location. The switch then issues RARPs for all the VLAN/MAC entries in the table.

Enabling this feature prevents possible traffic loss during vMotion in the following cases:

- the vNic is in VLAN trunk mode
- the VM is using more than one unicast MAC address. Etherswitch supports one unicast MAC per vNic, so only one RARP is sent.

8 Click **OK**.

What to do next

Click the logical switch in the Name column to view the logical switch details.

Connect a Logical Switch to an NSX Edge

Connecting a Logical Switch to an NSX Edge services gateway or an NSX Edge logical router provides East-West traffic routing (among the logical switches) or North-South traffic routing to the external world or to provide advanced services.

Procedure

1 In Logical Switches, select the logical switch to which you want to connect an NSX Edge.

2 Click the **Add Edge Gateway** () icon.

3 Select the NSX Edge to which you want to connect the logical switch and click **Next**.

4 Select the interface that you want to connect to the logical switch and click **Next**.

A logical network is typically connected to an internal interface.

5 On the Edit Edge Gateway Interface page, type a name for the NSX Edge interface.

6 Click **Internal** or **External** to indicate whether this is an internal or external interface.

7 Select the connectivity status of the interface.

8 If the NSX Edge to which you are connecting the logical switch has **Manual HA Configuration** selected, specify two management IP addresses in CIDR format.

9 Edit the default MTU if required.

10 Click **Next**.

11 Review the NSX Edge connection details and click **Finish**.

Deploy Services on a Logical Switch

You can deploy third party services on a Logical Switch.

Prerequisites

One or more third party virtual appliances must have been installed in your infrastructure.

Procedure

1 In **Logical Switches**, select the logical switch on which you want to deploy services.

2 Click the **Add Service Profile** ( ) icon.

3 Select the service and service profile that you want to apply.

4 Click **OK**.

Connect Virtual Machines to a Logical Switch

You can connect virtual machines to a Logical Switch. This makes it easy to identify the port groups that belong to a Logical Switch in your vCenter inventory.

Procedure

1 In **Logical Switches**, select the Logical Switch to which you want to add virtual machines.

2 Click the **Add** ( ) icon.

3 Select the vNics that you want to connect.

4 Click **Next**.

5 Review the vNics you selected.

6 Click **Finish**.

Test Logical Switch Connectivity

A ping test checks if two hosts in a VXLAN transport network can reach each other.

1 In **Logical Switches**, click the logical network that you want to test in the **Name** column.

2 Click the **Hosts** tab.

3 Select a host.

4 Click the **More Actions** ( ) icon and select **Test Connectivity**.

The Test Connectivity Between Hosts in the Network dialog box opens. The host you selected in step 4 appears in the Source host field. Click **Browse** to select a different source host.

5 Select the size of the test packet.

VXLAN standard size is 1550 bytes (should match the physical infrastructure MTU) without fragmentation. This allows NSX to check connectivity and verify that the infrastructure is prepared for VXLAN traffic.

Minimum packet size allows fragmentation. Hence, with packet size minimized, NSX can check connectivity but not whether the infrastructure is ready for the larger frame size.

6 In the **Destination** panel, click **Browse Hosts**.

7 In the Select Host dialog box, select the destination host.

8 Click **Select**.

9 Click **Start Test**.

The host-to-host ping test results are displayed.

Prevent Spoofing on a Logical Switch

After synchronizing with the vCenter Server, NSX Manager collects the IP addresses of all vCenter guest virtual machines from VMware Tools on each virtual machine. NSX does not trust all IP addresses provided by VMware Tools on a virtual machine. If a virtual machine has been compromised, the IP address can be spoofed and malicious transmissions can bypass firewall policies.

SpoofGuard allows you to authorize the IP addresses reported by VMware Tools, and alter them if necessary to prevent spoofing. SpoofGuard inherently trusts the MAC addresses of virtual machines collected from the VMX files and vSphere SDK. Operating separately from the Firewall rules, you can use SpoofGuard to block traffic identified as spoofed.

For more information, see "Using SpoofGuard," on page 53.

Edit a Logical Switch

You can edit the name, description, and control plane mode of a logical switch.

Procedure

1 In **Logical Switches**, select the logical switch that you want to edit.

2 Click the **Edit** icon.

3 Make the desired changes.

4 Click **OK**.

Working with Transport Zones

Add a Transport Zone

A transport zone defines the span of a logical switch. It can span one or more vSphere clusters. An NSX environment can contain one or more transport zones based on your requirements.

If a vDS spans more than one cluster and the transport zone is based on one of these clusters, the logical switch associated with this transport zone can access virtual machines within all clusters spanned by the vDS. In other words, this transport zone will not be able to constrain the logical switch span to a single cluster.

If this logical switch is later connected to a distributed router, you must ensure that the router instances are created only in the cluster included in the transport zone to avoid any Layer 3 issues.

Procedure

1 In the vSphere Web Client, click **Networking & Security > Installation**.

2 Click **Logical Network Preparation** and then click **Transport Zones**.

3 Click the **New Transport Zone** icon.

4 In the New Transport Zone dialog box, type a name and description for the transport zone.

5 Depending on whether you have a controller node in your environment, or you want to use multicast addresses, select the control plane mode.

- **Multicast**: Multicast IP addresses in the physical network are used for the control plane. This mode is recommended only when you are upgrading from older VXLAN deployments. Requires PIM/IGMP in the physical network.
- **Unicast** : The control plane is handled by an NSX controller. All unicast traffic leverages headend replication. No multicast IP addresses or special network configuration is required.
- **Hybrid** : The optimized unicast mode. Offloads local traffic replication to the physical network (L2 multicast). This requires IGMP snooping on the first-hop switch, but does not require PIM. The first-hop switch handles traffic replication for the subnet.

6 Select the clusters to be added to the transport zone.

7 Click **OK**.

View and Edit a Transport Zone

You can view the logical networks in a selected transport zone, the clusters in, and the control plane mode for that transport zone.

Procedure

1 In Transport Zones, double-click a transport zone.

The Summary tab displays the name and description of the transport zone as well as the number of logical switches associated with it. Transport Zone Details displays the clusters in the transport zone.

2 Click the **Edit Settings** icon in the **Transport Zone Details** section to edit the name, description, or control plane mode of the transport zone.

If you change the transport zone control plane mode, select **Migrate existing Logical Switches to the new control plane mode** to change the control plane more for existing logical switches linked to this transport zone. If you do not select this check box, only the logical switches linked to this transport zone after the edit is done will have the new control plane mode.

3 Click **OK**.

Expand a Transport Zone

You can add clusters to a transport zone. All existing transport zones become available on the newly added clusters.

Prerequisites

The clusters you add to a transport zone have the network infrastructure installed and are configured for VXLAN. See the *NSX Installation and Upgrade Guide*.

Procedure

1 In Transport Zones, click a transport zone.

2 In Transport Zones Details, click the **Add Cluster** () icon.

3 Select the clusters you want to add to the transport zone.

4 Click **OK**.

Contract a Transport Zone

You can remove clusters from a transport zone. The size of existing transport zones is reduced to accommodate the contracted scope.

Procedure

1 In **Transport Zones**, double-click a transport zone.

2 In **Transport Zones Details**, click the **Remove Clusters** ( ) icon.

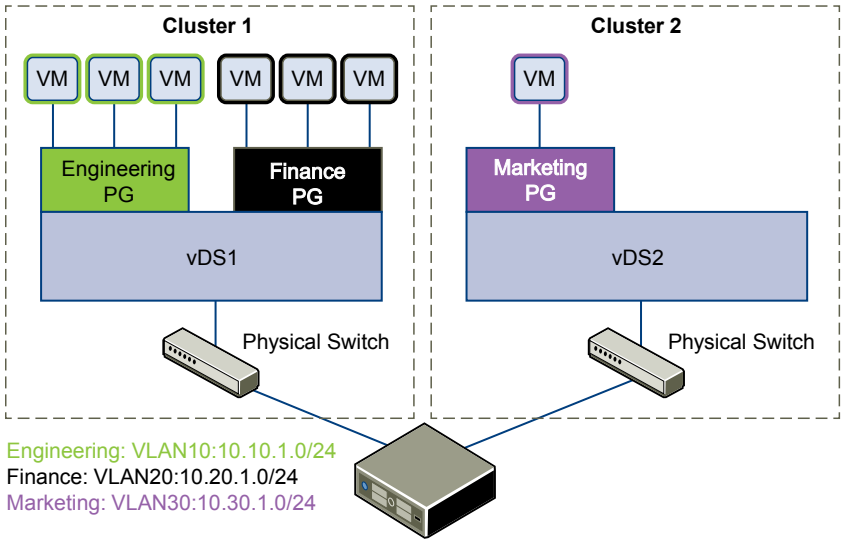
3 Select the clusters that you want to remove.

4 Click **OK**.

Logical Switch Scenario

This scenario presents a situation where company ACME Enterprise has several ESX hosts on two clusters in a datacenter, ACME_Datacenter. The Engineering (on port group PG-Engineering) and Finance departments (on port group PG-Finance) are on Cluster1. The Marketing department (PG-Marketing) is on Cluster2. Both clusters are managed by a single vCenter Server 5.5.

Figure 2-1. ACME Enterprise network before implementing logical switches

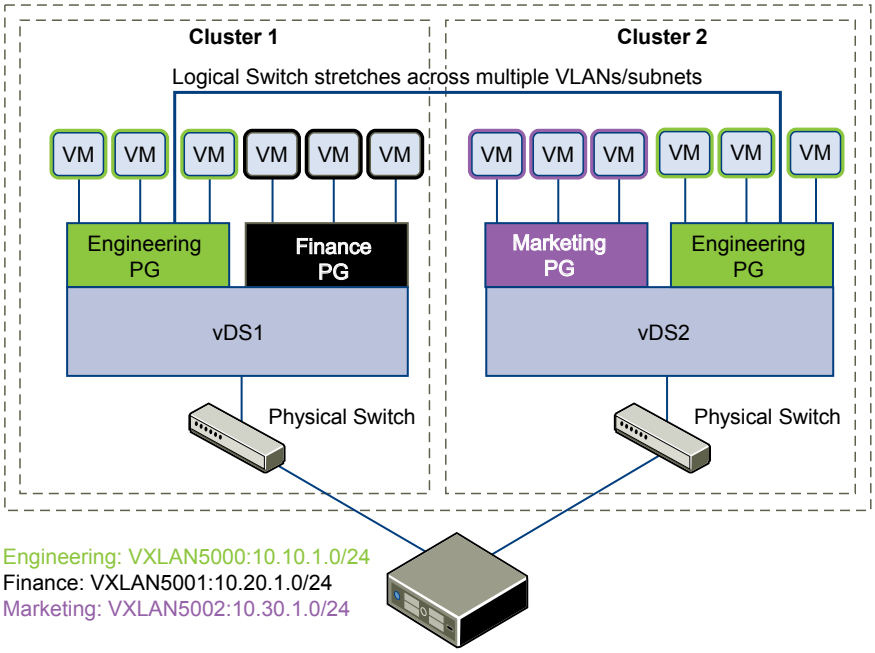


ACME is running out of compute space on Cluster1 while Cluster2 is under-utilized. The ACME network supervisor asks John Admin (ACME's virtualization administrator) to figure out a way to extend the Engineering department to Cluster2 in a way that virtual machines belonging to Engineering on both clusters can communicate with each other. This would enable ACME to utilize the compute capacity of both clusters by stretching ACME's L2 layer.

If John Admin were to do this the traditional way, he would need to connect the separate VLANs in a special way so that the two clusters can be in the same L2 domain. This might require ACME to buy a new physical device to separate traffic, and lead to issues such as VLAN sprawl, network loops, and administration and management overhead.

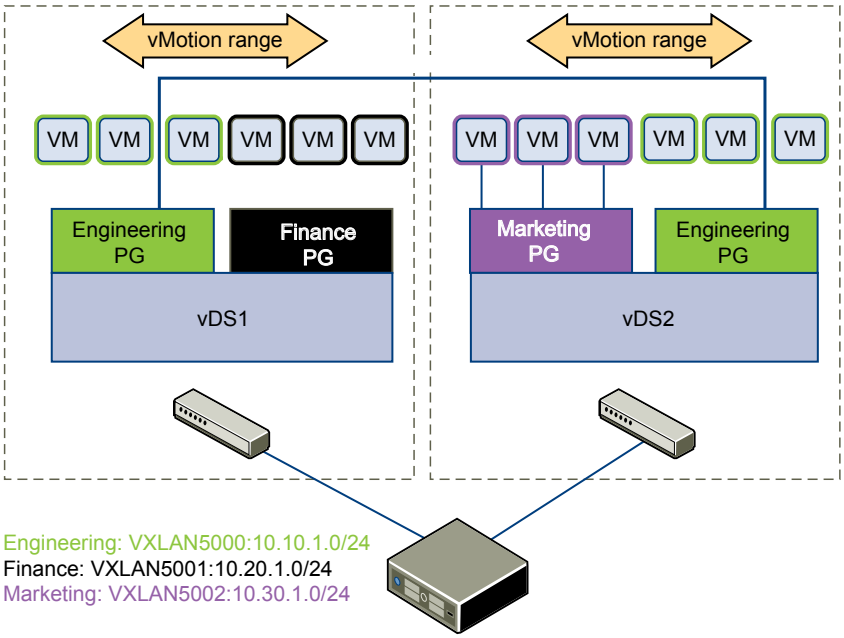
John Admin remembers seeing a logical network demo at VMworld, and decides to evaluate NSX. He concludes that building a logical switch across dvSwitch1 and dvSwitch2 will allow him to stretch ACME's L2 layer. Since John can leverage the NSX controller, he will not have to touch ACME's physical infrastructure as NSX works on top of existing IP networks.

Figure 2-2. ACME Enterprise implements a logical switch



Once John Admin builds a logical switch across the two clusters, he can vMotion virtual machines within the vDS.

Figure 2-3. vMotion on a logical network



Let us walk through the steps that John Admin follows to build a logical network at ACME Enterprise.

John Admin Assigns Segment ID Pool and Multicast Address Range to NSX Manager

John Admin must specify the segment ID pool he received to isolate Company ABC's network traffic.

Prerequisites

1 John Admin verifies that dvSwitch1 and dvSwitch2 are VMware distributed switches version 5.5.

2 John Admin sets the Managed IP address for the vCenter Server.

   a Select **Administration > vCenter Server Settings > Runtime Settings**.

   b In vCenter Server Managed IP, type **`10.115.198.165`**.

   c Click **OK**.

3 John Admin installs the network virtualization components on Cluster1 and Cluster 2. See *NSX Installation and Upgrade Guide*.

4 John Admin gets a segment ID pool (5000 - 5250) from ACME's NSX Manager administrator. Since he is leveraging the NSX controller, he does not require multicast in his physical network.

5 John Admin creates an IP pool so that he can assign a static IP address to the VXLAN VTEPs from this IP pool. See "Add an IP Pool," on page 67.

Procedure

1 In the vSphere Web Client, click **Networking & Security > Installation**.

2 Click the **Logical Network Preparation** tab and then click **Segment ID**.

3 Click **Edit**.

4 In Segment ID pool, type **`5000 – 5250`**.

5 Do not select **Enable multicast addressing**.

6 Click **OK**.

John Admin Configures VXLAN Transport Parameters

John Admin configures VXLAN on Cluster 1 and Cluster 2, where he maps each cluster to a vDS. When he maps a cluster to a switch, each host in that cluster is enabled for logical switches.

Procedure

1 Click the **Host Preparation** tab.

2 For Cluster1, select **Configure** in the VXLAN column.

3 In the Configuring VXLAN networking dialog box, select dvSwitch1 as the virtual distributed switch for the cluster.

4 Type **`10`** for dvSwitch1 to use as the ACME transport VLAN.

5 In Specify Transport Attributes, leave 1600 as the Maximum Transmission Units (MTU) for dvSwitch1.

   MTU is the maximum amount of data that can be transmitted in one packet before it is divided into smaller packets. John Admin knows that VXLAN logical switch traffic frames are slightly larger in size because of the encapsulation, so the MTU for each switch must be set to 1550 or higher.

6 In **VMKNic IP Addressing**, select **Use IP Pool** and select an IP pool.

7 For **VMKNic Teaming Policy**, select **Failover**.

John Admin wants to maintain the quality of service in his network by keeping the performance of logical switches the same in normal and fault conditions. Hence, he chooses Failover as the teaming policy.

8 Click **Add**.

9 Repeat steps 4 through step 8 to configure VXLAN on Cluster2.

After John admin maps Cluster1 and Cluster2 to the appropriate switch, the hosts on those clusters are prepared for logical switches:

1 A VXLAN kernel module and vmknic is added to each host in Cluster 1 and Cluster 2.

2 A special dvPortGroup is created on the vSwitch associated with the logical switch and the VMKNic is connected to it.

John Admin Adds a Transport Zone

The physical network backing a logical network is called a transport zone. A transport zone is the compute diameter spanned by a virtualized network.

Procedure

1 Click **Logical Network Preparation** and then click **Transport Zones**.

2 Click the **New Transport Zone** icon.

3 In Name, type **ACME Zone**.

4 In Description, type **Zone containing ACME's clusters**.

5 Select Cluster 1 and Cluster 2 to add to the transport zone.

6 In **Control Plane Mode**, select **Unicast**.

7 Click **OK**.

John Admin Creates a Logical Switch

After John Admin configures VXLAN transport parameters, he is ready to create a logical switch.

Procedure

1 Click **Logical Switches** and then click the **New Logical Network** icon.

2 In Name, type **`ACME logical network`**.

3 In Description, type **`Logical Network for extending ACME Engineering network to Cluster2`**.

4 In **Transport Zone**, select ACME Zone.

5 Click **OK**.

NSX creates a logical switch providing L2 connectivity between dvSwitch1 and dvSwitch2.

What to do next

John Admin can now connect ACME's production virtual machines to the logical switch, and connect the logical switch to an NSX Edge services gateway or Logical Router.

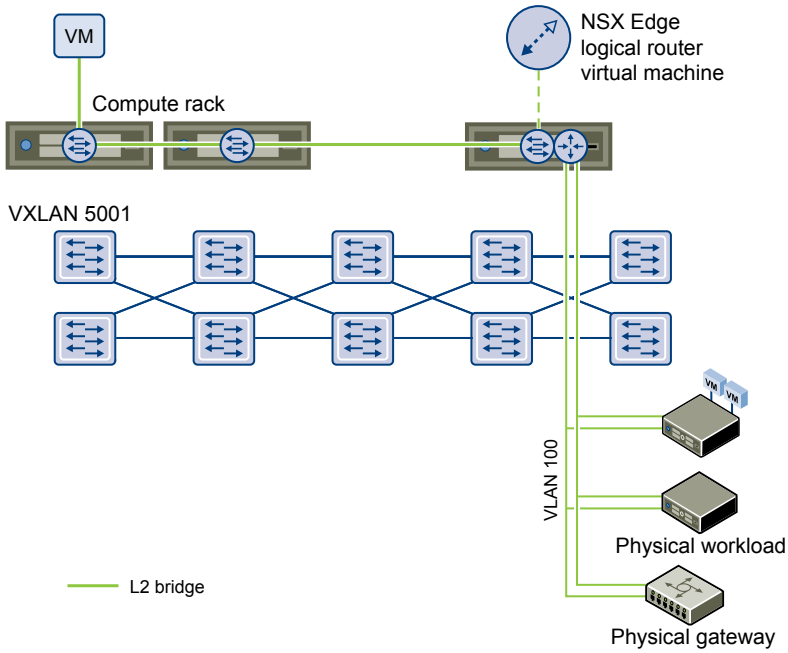
L2 Bridges

3

You can create an L2 bridge between a logical switch and a VLAN, which enables you to migrate virtual workloads to physical devices with no impact on IP addresses. A logical network can leverage a physical L3 gateway and access existing physical networks and security resources by bridging the logical switch broadcast domain to the VLAN broadcast domain.

The L2 bridge runs on the host that has the NSX Edge logical router virtual machine. An L2 bridge instance maps to a single VLAN, but there can be multiple bridge instances. The logical router cannot be used as a gateway for devices connected to a bridge.

If High Availability is enabled on the Logical Router and the primary NSX Edge virtual machine goes down, the bridge is automatically moved over to the host with the secondary virtual machine. For this seamless migration to happen, a VLAN must have been configured on the host that has the secondary NSX Edge virtual machine.



Note that you should not use an L2 bridge to connect a logical switch to another logical switch, a VLAN network to another VLAN network, or to interconnect datacenters.

Add L2 Bridge

You can add a bridge from a logical switch to a distributed virtual port group.

Prerequisites

An NSX logical router must be deployed in your environment.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click **Bridging**.

5 Click the **Add** icon.

6 Type a name for the bridge.

7 Select the logical switch that you want to create a bridge for.

8 Select the distributed virtual port group to which you want to bridge the logical switch.

9 Click **OK**.

Logical Router 4

You can specify static and dynamic routing for each NSX Edge.

Dynamic routing provides the necessary forwarding information between Layer 2 broadcast domains, thereby allowing you to decrease Layer 2 broadcast domains and improve network efficiency and scale. NSX extends this intelligence to where the workloads reside for doing East-West routing. This allows more direct virtual machine to virtual machine communication without the added cost or time needed to extend hops. At the same time, NSX also provides North-South connectivity, thereby enabling tenants to access public networks.

This chapter includes the following topics:

- "Specify Global Configuration," on page 33
- "Add a Static Route," on page 34
- "Configure OSPF," on page 35
- "Configure BGP," on page 36
- "Configure IS-IS Protocol," on page 37
- "Configure Route Redistribution," on page 38

Specify Global Configuration

You can configure the default gateway for static routes and specify dynamic routing details for an Edge Services Gateway or Distributed Router.

You must have a working NSX Edge instance before you can configure routing on it. For information on setting up NSX Edge, see "NSX Edge Operations," on page 166.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Routing** and then click **Global Configuration**.

5 To enable Equal-cost multi-path routing (ECMP), click **Enable** next to ECMP.

ECMP is a routing strategy that allows next-hop packet forwarding to a single destination can occur over multiple best paths. These best paths can be added statically or as a result of metric calculations by dynamic routing protocols like OSPF or BGP. Multiple paths for static routes can be added by providing multiple next hops separated by commas in the Static Routes dialog box. For more information, see "Add a Static Route," on page 34.

The Edge Services Gateway utilizes Linux network stack implementation, a roundrobin algorithm with a randomness component. After a next hop is selected for a particular source and destination IP address pair, the route cache stores the selected next hop. All packets for that flow go to the selected next hop. The default IPv4 route cache timeout is 300 seconds (gc_timeout). If an entry is inactive for this time, it is eligible to be removed from the route cache. The actual removal happens when garbage collection timer activates (gc_interval = 60 seconds).

The Logical Router uses an XOR algorithm to determine the next hop from a list of possible ECMP next hops. This algorithm uses the source and destination IP address on the outgoing packet as sources of entropy.

Enabling ECMP disables firewall on the Edge Services Gateway virtual machine. Stateful services such as NAT do not work with ECMP.

6 To specify the default gateway, click **Edit** next to **Default Gateway**.

   a Select an interface from which the next hop towards the destination network can be reached.

   b Type the gateway IP if required.

   c Edit the MTU if required and type a description.

   d Click **Save**.

7 To configure dynamic routing, click **Edit** next to Dynamic Routing Configuration.

   a **Router ID** uniquely identifies the peer that is sending routes. Select an external interface whose IP address you want to use as the Router ID, or select **Custom ID** and type an IP address.

   b Do not enable any protocols here.

   c Select **Enable Logging** to save logging information and select the log level.

8 Click **Publish Changes**.

What to do next

To delete routing configuration, click **Reset**. This deletes all routing configurations (default, static, OSPF, and BGP configurations, as well as route redistribution).

Add a Static Route

You can add a static route for a destination subnet or host.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **Routing** tab.

5 Select **Static Routes** from the left panel.

6 Click the **Add** () icon.

7 Type a description for the static route.

8 Select the interface on which you want to add a static route.

9 Type the **Network** in CIDR notation.

10 Type the IP address of the **Next Hop**.

   The router must be able to directly reach the next hop.

11 For MTU, edit the maximum transmission value for the data packets if required.

The MTU cannot be higher than the MTU set on the NSX Edge interface.

12 Click **OK**.

Configure OSPF

NSX Edge supports OSPF, an interior gateway protocol that routes IP packets only within a single routing domain. It gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer, which makes routing decisions based on the destination IP address found in IP packets.

OSPF routing policies provide a dynamic process of traffic load balancing between routes of equal cost.

An OSPF network is divided into routing areas to optimize traffic flow and limit the size of routing tables. An area is a logical collection of OSPF networks, routers, and links that have the same area identification.

Areas are identified by an Area ID.

Prerequisites

Router ID must have been specified. See "Specify Global Configuration," on page 33.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Routing** and then click **OSPF**.

5 Do one of the following.

Option	Description
For an Edge services gateway	Click **Enable**.
For a logical router	a Click **Edit** at the top right corner of the window. b Click **Enable OSPF**. c In **Forwarding Address**, type an IP address that is to be used by the router datapath module in the hosts to forward datapath packets. d In **Protocol Address**, type a unique IP address within the same subnet as the **Forwarding Address**. Protocol address is used by the protocol to form adjacencies with the peers.

6 In **Area Definitions**, click the **Add** icon.

7 Type an Area ID. NSX Edge supports an area ID in the form of an IP address or decimal number.

8 Select **Stub** in the **Type** field. Typically, there is no hierarchical routing beyond the stub.

9 Select the type of **Authentication**. OSPF performs authentication at the area level. Hence, all routers within the area must have the same authentication and corresponding password configured. For MD5 authentication to work, both the receiving and transmitting routers must have the same MD5 key.

a **None**: No authentication is required, which is the default value.

b **Password**: In this method of authentication, a password is included in the transmitted packet.

c **MD5**: This authentication method uses MD5 (Message Digest type 5) encryption. An MD5 checksum is included in the transmitted packet.

10 For **Password** or **MD5** type authentication, type the password or MD5 key.

11 Click **OK**.

12 In **Area to Interface Mapping**, click the **Add** icon to map the interface that belongs to the OSPF area.

13 Select the interface that you want to map and the OSPF area that you want to map it to.

14 **Hello Interval** displays the default interval between hello packets that are sent on the interface. Edit the default value if required.

15 **Dead Interval** displays the default interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down. Edit the default interval if required.

16 **Priority** displays the default priority of the interface. The interface with the highest priority is the designated router. Edit the default value if required.

17 **Cost** of an interface displays the default overhead required to send packets across that interface. The cost of an interface is inversely proportional to the bandwidth of that interface. The larger the bandwidth, the smaller the cost. Edit the default value if required.

18 Click OK and then click **Publish Changes**.

Configure BGP

Border Gateway Protocol (BGP) makes core routing decisions. It includes a table of IP networks or prefixes, which designate network reachability among multiple autonomous systems.

An underlying connection between two BGP speakers is established before any routing information is exchanged. Keepalive messages are sent by the BGP speakers in order to keep this relationship alive. After the connection is established, the BGP speakers exchange routes and synchronize their tables.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Routing** and then click **BGP**.

5 Click **Edit**.

6 In the Edit BGP Configuration dialog box, click **Enable BGP**.

7 Type the router ID in **Local AS**. Type the Local AS. This is advertised when BGP peers with routers in other autonomous systems (AS). The path of ASs that a route traverses is used as one metric when selecting the best path to a destination.

8 Click **Save**.

9 In **Neighbors**, click the **Add** icon.

10 Type the IP address of the neighbor.

11 Type the remote AS.

12 Edit the default weight for the neighbor connection if required.

13 **Hold Down Timer** displays interval (180 seconds) after not receiving a keep alive message that the software declares a peer dead. Edit if required.

14 **Keep Alive Timer** displays the default frequency (60 seconds) with which the software sends keepalive messages to its peer. Edit if required.

15 If authentication is required, type the authentication password. Each segment sent on the connection between the neighbors is verified. MD5 authentication must be configured with the same password on both BGP neighbors, otherwise, the connection between them will not be made.

16 To specify route filtering from a neighbor, click the **Add** icon in the **BGP Filters** area.

CAUTION A "block all" rule is enforced at the end of the filters.

17 Select the direction to indicate whether you are filtering traffic to or from the neighbor.

18 Select the action to indicate whether you are allowing or denying traffic.

19 Type the network in CIDR format that you want to filter to or from the neighbor.

20 Type the IP prefixes that are to be filtered and click **OK**.

21 Click **Publish Changes**.

Configure IS-IS Protocol

Intermediate System to Intermediate System (IS-IS) is a routing protocol designed to move information by determining the best route for datagrams through a packet-switched network.

A two-level hierarchy is used to support large routing domains. A large domain may be divided into areas. Routing within an area is referred to as Level 1 routing. Routing between areas is referred to as Level 2 routing. A Level 2 Intermediate System (IS) keeps track of the paths to destination areas. A Level 1 IS keeps track of the routing within its own area. For a packet going to another area, a Level 1 IS sends the packet to the nearest Level 2 IS in its own area, regardless of what the destination area is. Then the packet travels via Level 2 routing to the destination area, where it may travel via Level 1 routing to the destination. An IS in both Level 1 and Level 2 is referred to as Level-1-2.

NOTE NSX support for the IS-IS protocol is currently experimental.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Routing** and then click **IS-IS**.

5 Click **Edit** and then click **Enable IS-IS**.

6 Type the System ID and select the IS-IS type.

Level 1 is intra-area, Level 2 is inter-area, and Level 1-2 is both. Level 2 routers are inter-area routers that can only form relationships with other Level 2 routers. Routing information is exchanged between Level 1 routers and other Level 1 routers. Likewise Level 2 routers only exchange information with other Level 2 routers. Level 1-2 routers exchange information with both levels and are used to connect the inter-area routers with the intra-area routers.

7 Type the **Domain Password** and **Area Password**. The area password is inserted and checked for Level 1 link state packets, and the domain password for Level 2 link state packets.

8 Define the IS-IS areas.

a Click the **Add** icon in **Areas**.

b Type up to three area IP addresses.

c Click **Save**.

9 Configure interface mapping.

a Click the **Add** icon in **Interface Mapping**.

b Choose the Circuit Type to indicate whether you are configuring the interface for Level-1, Level-2, or Level-1-2 adjacency.

c **Hello Interval** displays the default interval in milliseconds between hello packets that are sent on the interface. Edit the default value if required.

d **Hello Multiplier** displays the default number of IS-IS hello packets a neighbor must miss before it is declared down. Edit the default value if required.

e **LSP Interval** displays the time delay in milliseconds between successive IS-IS link-state packet (LSP) transmissions. Edit the default value if required.

f **Metric** displays the default metric for the interface. This is used to calculate the cost from each interface via the links in the network to other destinations. Edit the default value if required.

g **Priority** displays the priority of the interface. The interface with the highest priority becomes the designated router. Edit the default value if required.

h In Mesh Group, type the number identifying the mesh group to which this interface belongs. Edit the default value if required.

i Type the authentication password for the interface and click **OK**. Edit the default value if required.

10 **Click Publish Changes**.

Configure Route Redistribution

By default, routers share routes with other routers running the same protocol. In a multi-protocol environment, you must configure route redistribution for cross-protocol route sharing.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Routing** and then click **Route Redistribution**.

5 Click **Change** next to **Route Redistribution Status**.

6 Select the protocols for which you enable route redistribution and click **OK**.

7 Add an IP prefix.

Entries in the IP Prefix list are processed sequentially.

a Click the **Add** icon in **IP Prefixes**.

b Type a name and IP address of the network.

c Click **OK**.

8 Specify redistribution criteria for the IP prefix.

a Click the **Add** icon in **Route Redistribution table**.

b In **Learner Protocol**, select the protocol that is to learn routes from other protocols.

c In **Allow Learning from**, select the protocols from which routes should be learned.

d Click **OK**.

9 Click **Publish Changes**.

Logical Firewall 5

Logical Firewall provides security mechanisms for dynamic virtual data centers, and consists of two components to address different deployment use cases. Distributed Firewall focuses on East-West access controls, and Edge Firewall focuses on the North-South traffic enforcement at the tenant or datacenter perimeter. Together, these components address the end-to-end firewall needs of virtual datacenters. You can choose to deploy either of these technologies independently, or deploy both of them.

This chapter includes the following topics:

- "Distributed Firewall," on page 41
- "Edge Firewall," on page 42
- "Working with Firewall Rules," on page 42
- "Working with Firewall Rule Sections," on page 50
- "Working with Firewall Configurations," on page 51
- "Excluding Virtual Machines from Firewall Protection," on page 52
- "Using SpoofGuard," on page 53
- "View Firewall CPU and Memory Threshold Events," on page 56
- "Firewall Logs," on page 56
- "Working with Local Rules," on page 56

Distributed Firewall

Distributed Firewall is a hypervisor kernel-embedded firewall that provides visibility and control for virtualized workloads and networks. You can create access control policies based on VMware vCenter objects like datacenters and clusters and virtual machine names; network constructs like IP or IPSet addresses, VLAN (DVS port-groups), VXLAN (logical switches), security groups, as well as user group identity from Active Directory. Firewall rules are enforced at the vNIC level of each virtual machine to provide consistent access control even when the virtual machine gets vMotioned. The hypervisor-embedded nature of the firewall delivers close to line rate throughput to enable higher workload consolidation on physical servers. The distributed nature of the firewall provides a scale-out architecture that automatically extends firewall capacity when additional hosts are added to a datacenter.

For L2 packets, Distributed Firewall creates a cache for performance boost. L3 packets are processed in the following sequence:

1. All packets are checked for an existing state. This is done for SYNs too so that bogus or retransmitted SYNs for existing sessions can be detected.
2. If a state match is found, the packets are processed.

3 If a state match is not found, the packet is processed through the rules until a match is found.

- For TCP packets, a state is set only for packets with a SYN flag. However, rules that do not specify a protocol (service ANY), can match TCP packets with any combination of flags.
- For UDP packets, 5-tuple details are extracted from the packet. If a state does not exist in the state table, a new state is created using the extracted 5-tuple details. Subsequently received packets are matched against the state that was just created.
- For ICMP packets, ICMP type, code, and packet direction are used to create a state.

Distributed Firewall can help in creating identity-based rules as well. Administrators can enforce access control based on the user's group membership as defined in the enterprise Active Directory. Here are some scenarios where identity-based firewall rules can be used:

- User accessing virtual applications using a laptop or mobile device where AD is used for user authentication
- User accessing virtual applications using VDI infrastructure where the virtual machines are Microsoft Windows based

If you have a third-party vendor firewall solution deployed in your environment, see "Redirecting Traffic to a Vendor Solution through Logical Firewall," on page 141.

Edge Firewall

Edge Firewall monitors North-South traffic to provide perimeter security functionality including firewall, Network Address Translation (NAT) as well as site-to-site IPSec and SSL VPN functionality. This solution is available in the virtual machine form factor and can be deployed in a High Availability mode.

Working with Firewall Rules

Distributed Firewall rules and Edge Firewall rules can be managed in a centralized manner on the Firewall tab. In a multi-tenant environment, providers can define high-level traffic flow rules on the centralized Firewall user interface. Rules defined on the centralized level are referred to as pre rules. Tenants can then add rules at an individual NSX Edge level, which are referred to as local rules.

Each traffic session is checked against the top rule in the Firewall table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced. Rules are displayed in the following order:

1 User-defined pre rules have the highest priority, and are enforced in top-to-bottom ordering with a per-virtual NIC level precedence.

2 Auto-plumbed rules (rules that enable control traffic to flow for Edge services).

3 Local rules defined at an NSX Edge level.

4 Service Composer rules - a separate section for each policy. You cannot edit these rules in the Firewall table, but you can add rules at the top of a security policy firewall rules section. If you do so, you must re-synchronize the rules in Service Composer. For more information, see Chapter 9, "Service Composer," on page 115.

5 Default Distributed Firewall rules

Note that firewall rules are enforced only on clusters on which you have enabled firewall. For information on preparing clusters, see the *NSX Installation and Upgrade Guide*.

Edit the Default Distributed Firewall Rule

Default firewall settings apply to traffic that does not match any of the user-defined firewall rules. The Distributed Firewall default rule is displayed on the centralized firewall user interface, and the default rule for each NSX Edge is displayed at the NSX Edge level.

The default Distributed Firewall rule allows all L3 and L2 traffic to pass through all prepared clusters in your infrastructure. The default rule is always at the bottom of the rules table and cannot be deleted or added to. However, you can change the Action element of the rule from Allow to Block or Reject, add comments for the rule, and indicate whether traffic for that rule should be logged.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > Firewall**.

2 Expand the Default Section and make the required changes.

You can only edit **Action** and **Log**, or add comments to the default rule.

Add a Firewall Rule

You add firewall rules at the global scope. Using the Applied To field, you can then narrow down the scope at which you want to apply the rule. Firewall allows you to add multiple objects at the source and destination levels for each rule, which helps reduce the total number of firewall rules to be added.

The following vCenter objects can be specified as the source or destination for a firewall rule:

- cluster
- datacenter
- distributed port group
- IP set
- legacy port group
- logical switch
- resource pool
- security group
- vApp
- virtual machine
- vNIC
- IP address (IPv4 or IPv6)

The following objects can be used in the AppliedTo field to narrow the scope of a firewall rule.

- All clusters on which Distributed Firewall has been installed (in other words, all clusters that have been prepared for network virtualization)
- All Edge gateways
- cluster
- datacenter
- distributed port group
- Edge
- legacy port group

- logical switch
- virtual machine
- vNIC

Prerequisites

If you are adding an identity-based firewall rule, ensure that:

- One or more domains have been registered with NSX Manager. NSX Manager gets group and user information as well as the relationship between them from each domain that it is registered with. See "Register a Windows Domain with NSX Manager," on page 164.
- A security group based on Active Directory objects has been created which can be used as the source or destination of the rule. See "Create a Security Group," on page 152.

If you are adding a rule based on a VMware vCenter object, ensure that VMware Tools is installed on the virtual machines. See *NSX Installation and Upgrade Guide*.

Procedure

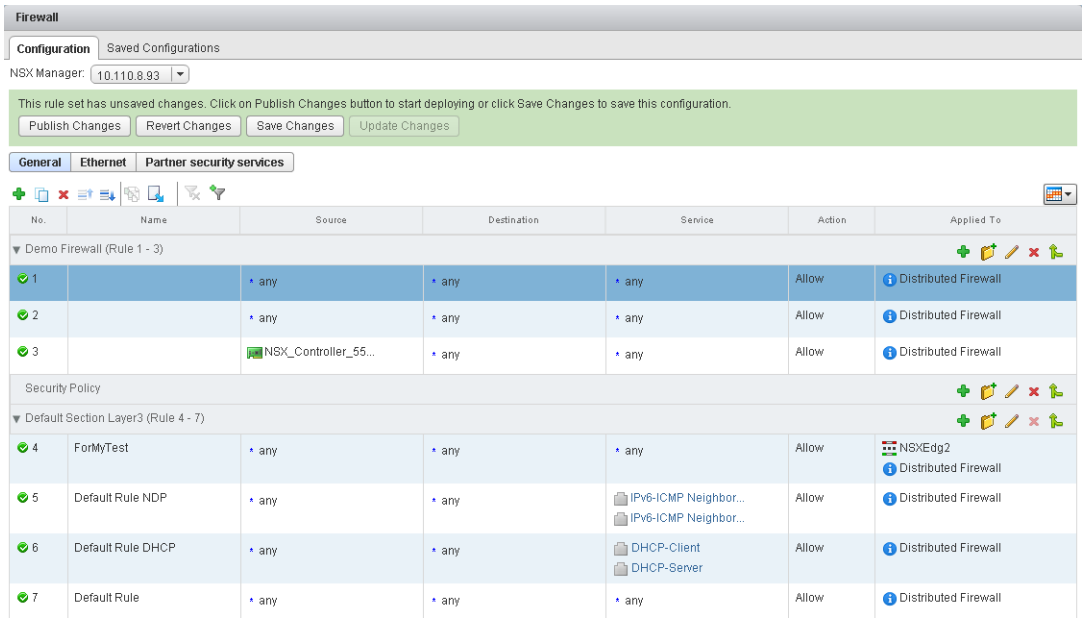
1 In the vSphere Web Client, navigate to **Networking & Security > Firewall**.

2 Ensure that you are in the **General** tab to add an L3 rule. Click the **Ethernet** tab to add an L2 rule.

3 In the section in which you add a rule, click **Add rule** ( ) icon.

A new any any allow rule is added at the top of the section. If the system-defined rule is the only rule in the section, the new rule is added above the default rule.

If you want to add a rule at a specific place in a section, select a rule. In the No. column, click and select **Add Above** or **Add Below**.



4 Point to the **Name** cell of the new rule and click .

5 Type a name for the new rule.

6 Point to the **Source** cell of the new rule. Additional icons are displayed as described in the table below.

Option	Description
Click IP	To specify source as an IP address. a Select the IP address format. Firewall supports both IPv4 and IPv6 formats. b Type the IP address.
Click ⊞	To specify source as an object other than a specific IP address. a In **View**, select a container from which the communication originated. Objects for the selected container are displayed. b Select one or more objects and click  . You can create a new security group or IPSet. Once you create the new object, it is added to the source column by default. For information on creating a new security group or IPSet, see Chapter 13, "Network and Security Objects," on page 149. c To specify a source port, click **Advance options** and type the port number or range. d Select **Negate Source** to exclude this source port from the rule. If **Negate Source** is selected, the rule applied to traffic coming from all sources except for the source you specified in the previous step. If **Negate Source** is not selected, the rule applies to traffic coming from the source you specified in the previous step. e Click **OK**.

7 Point to the **Destination** cell of the new rule. Additional icons are displayed as described in the table below.

Option	Description
Click IP	To specify destination as an IP address. a Select the IP address format. Firewall supports both IPv4 and IPv6 formats. b Type the IP address.
Click ⊞	To specify destination as an object other than a specific IP address. a In **View**, select a container which the communication is targeting. Objects for the selected container are displayed. b Select one or more objects and click  . You can create a new security group or IPSet. Once you create the new object, it is added to the Destination column by default. For information on creating a new security group or IPSet, see Chapter 13, "Network and Security Objects," on page 149. c To specify a destination port, click **Advance options** and type the port number or range. d Select **Negate Destination** to exclude this source port from the rule. If **Negate Destination** is selected, the rule applied to traffic going to all destinations except for the destination you specified in the previous step. If **Negate Destination** is not selected, the rule applies to traffic going to the destination you specified in the previous step. e Click **OK**.

8 Point to the **Service** cell of the new rule. Additional icons are displayed as described in the table below.

Option	Description
Click	To specify service as a port protocol combination. a Select the service protocol. Distributed Firewall supports ALG (Application Level Gateway) for the following protocols: FTP, CIFS, ORACLE TNS, MS-RPC, and SUN-RPC. Edge supports ALG for FTP only. b Type the port number and click **OK**.
Click	To select a pre-defined service/service group or define a new one. a Select one or more objects and click . You can create a new service or service group. Once you create the new object, it is added to the Destination column by default. b Click **OK**.

In order to protect your network from ACK or SYN floods, you can set Service to TCP-all_ports or UDP-all_ports and set Action to Block for the default rule. For information on modifying the default rule, see "Edit the Default Distributed Firewall Rule," on page 43.

9 Point to the **Action** cell of the new rule and click . Make appropriate selections as described in the table below and click **OK**.

Action	Results in
Allow	Allows traffic from or to the specified source(s), destination(s), and service(s).
Block	Blocks traffic from or to the specified source(s), destination(s), and service(s).
Reject	Sends reject message for unaccepted packets. RST packets are sent for TCP connections. ICMP messages with administratively prohibited code are sent for UDP, ICMP, and other IP connections.
Log	Logs all sessions matching this rule. Enabling logging can affect performance.
Do not log	Does not log sessions.

10 In **Applied To**, define the scope at which this rule is applicable. Make appropriate selections as described in the table below and click **OK**.

To apply a rule to	Do this
All prepared clusters in your environment	Select **Apply this rule on all clusters on which Distributed Firewall is enabled**. After you click OK, the Applied To column for this rule displays **Distributed Firewall**.
All NSX Edge gateways in your environment	Select **Apply this rule on all Edge gateways**. After you click OK, the Applied To column for this rule displays **All Edges**. If both the above options are selected, the Applied To column displays **Any**.
One or more cluster, datacenter, distributed virtual port group, NSX Edge, network, virtual machine, vNIC, or logical switch	1 In **Container type**, select the appropriate object.. 2 In the Available list, select one or more objects and click .

If the rule contains virtual machines/vNICS in the source and destination fields, you must add both the source and destination virtual machines/vNICS to **Applied To** for the rule to work correctly.

11 Click **Publish Changes**.

After a few moments, a message indicating whether the publish operation was successful is displayed. In case of any failures, the hosts on which the rule was not applied are listed. For additional details on a failed publish, navigate to **NSX Managers >** ***NSX_Manager_IP_Address*****Monitor > System Events**.

When you click **Publish Changes**, the firewall configuration is automatically saved. For information on reverting to an earlier configuration, see "Load Firewall Configuration," on page 52.

What to do next

- Disable a rule by clicking  , or enable a rule by clicking  .
- Display additional columns in the rule table by clicking  and selecting the appropriate columns.

Column Name	Information Displayed
Rule ID	Unique system generated ID for each rule
Log	Traffic for this rule is being logged or not
Stats	Clicking  shows the traffic related to this rule (traffic packets and size)
Comments	Comments for the rule

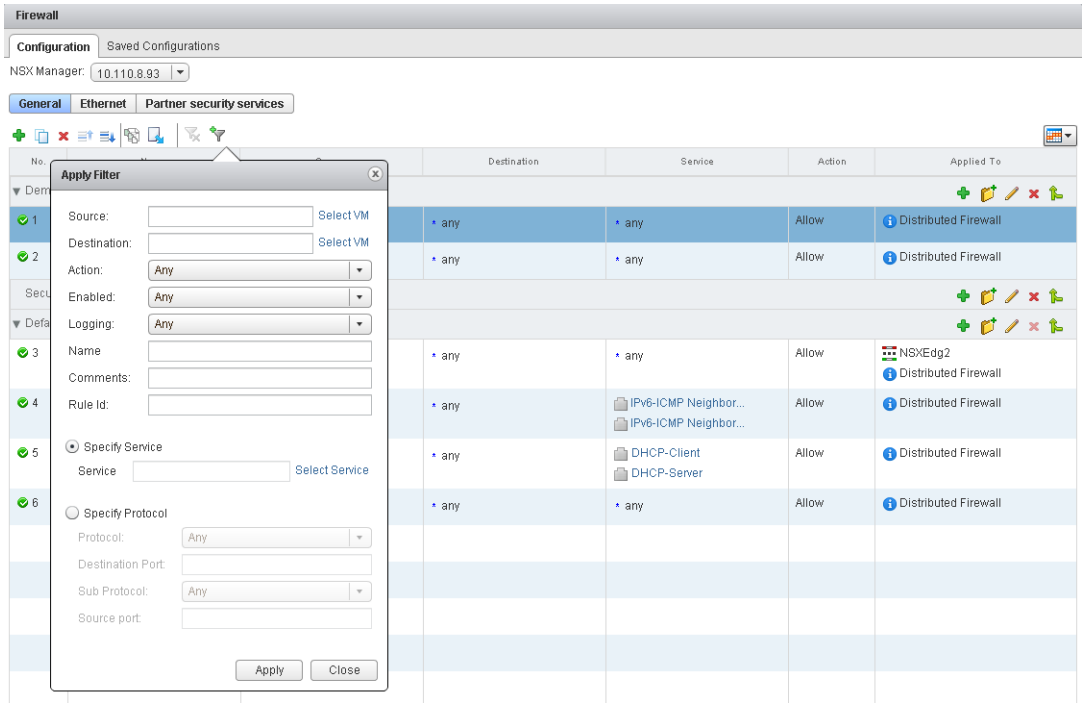
- Search for rules by typing text in the Search field.
- Move a rule up or down in the Firewall table.
- Merge sections by clicking the **Merge section** icon and selecting **Merge with above section** or **Merge with below section**.

Filter Firewall Rules

You can use a wide number of criteria to filter your ruleset, which allows for easy rule modification. Rules can be filtered by source or destination virtual machines or IP address, rule action, logging, rule name, comments, and rule ID.

Procedure

1 In the Firewall tab, click the **Apply Filter** ( ) icon.



2 Type or select the filtering criteria as appropriate.

3 Click **Apply**.

Rules matching your filtering criteria are displayed.

What to do next

To display all rules again, click the **Remove applied filter** ( ) icon.

Add a Rule and PublishIt at a Later Time

You can add a rule and save the configuration without publishing it. You can then load and publish the saved configuration at a later time.

Procedure

1 Add a firewall rule. See "Add a Firewall Rule," on page 43.

2 Click **Save Changes**.

3 Type a name and description for the configuration and click **OK**.

4 Click **Preserve Configuration** to preserve this change.

NSX can save up to 100 configurations. After this limit is exceeded, saved configurations marked with **Preserve Configuration** are preserved while older non-preserved configurations are deleted to make room for preserved configurations.

5 Do one of the following.

- Click **Revert Changes** to go back to the configuration that existed before you added the rule. When you want to publish the rule you just added, click the **Load Configuration** icon, select the rule that you saved in step 3 and click **OK**.
- Click **Update Changes** to continue adding rules.

Change the Order of a Firewall Rule

Firewall rules are applied in the order in which they exist in the rule table.

Rules are displayed (and enforced) in the following order:

1 User-defined pre rules have the highest priority and are enforced in top-to-bottom ordering with a per-virtual NIC level precedence.

2 Auto-plumbed rules.

3 Local rules defined at an NSX Edge level.

4 Service Composer rules - a separate section for each policy. You cannot edit these rules in the Firewall table, but you can add rules at the top of a security policy firewall rules section. If you do so, you must re-synchronize the rules in Service Composer. For more information, see Chapter 9, "Service Composer," on page 115.

5 Default Distributed Firewall rule

You can move a custom rule up or down in the table. The default rule is always at the bottom of the table and cannot be moved.

Procedure

1 In the **Firewall** tab, select the rule that you want to move.

2 Click the **Move rule up** ( ) or **Move rule down** ( ) icon.

3 Click **Publish Changes**.

Delete a Firewall Rule

You can delete firewall rules that you created. You cannot delete the default rule or rules managed by Service Composer.

Procedure

1 In the **Firewall** tab, select a rule.

2 Click **Delete selected rule** ( ) icon above the Firewall table.

3 Click **Publish Changes**.

Working with Firewall Rule Sections

You can add a section to segregate firewall rules. For example, you might want to have the rules for sales and engineering departments in separate sections.

Add a Firewall Rule Section

You can add a new section in the firewall table.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > Firewall**.

2 Ensure that you are in the **General** tab to add a section for L3 rules. Click the **Ethernet** tab to add a section for L2 rules.

3 Click the **Add Section** ( ) icon.

4 Type a name for the section and specify the position for the new section. Section names must be unique within NSX Manager.

5 Click **OK**.

What to do next

Add rules to the section. You can edit the name of a section by clicking the **Edit** icon for that section.

Merge Firewall Rule Sections

You can merge sections and consolidate the rules within those sections. Note that you cannot merge a Service Composer section or the Default section.

Merging and colidating a complex firewall configuration can help with maintenance and readability.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > Firewall**.

2 For the section you want to merge, click the **Merge** ( ) icon and specify whether you want to merge this section with the section above or below.

Rules from both sections are merged. The new section keeps the name of the section with which the other section is merged.

3 Click **Publish Changes**.

Delete a Firewall Rule Section

You can delete a firewall rule section. All rules in that section are deleted.

You cannot delete a section and add it again at a different place in the firewall table. To do so, you must delete the section and publish the configuration. Then add the deleted section to the firewall table and re-publish the configuration.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > Firewall**.

2 Ensure that you are in the **General** tab to delete a section for L3 rules. Click the **Ethernet** tab to delete a section for L2 rules.

3 Click the **Delete section** ( ) icon for the section you want to delete.

4 Click **OK** and then click **Publish Changes**.

The section as well as all rules in that section are deleted.

Working with Firewall Configurations

You can export your current firewall configuration and import this configuration into another NSX Manager.

Export Firewall Configuration

You can export your firewall configuration.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > Firewall**.

2 Click the **Export configuration** ( ) icon.

3 To save the firewall configuration as an XML file, click **Download**.

4 Select the directory where you want to save the file and click **Save**.

Your firewall configuration (both L2 and L3) is saved in the specified directory.

Import Firewall Configuration

You can import a saved configuration and then load it in the Firewall table. The imported configuration overwrites the existing rules. There is no way to import a partial set of rules.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > Firewall**.

2 Click the **Firewall** tab.

3 Click the **Saved Configurations** tab.

4 Click the **Import configuration** ( ) icon.

5 Click **Browse** and select the file containing the configuration that you want to import.

Rules are imported based on the rule names. During the import, Firewall ensures that each object referenced in the rule exists in your environment. If an object is not found, the rule is marked as invalid. If a rule references a dynamic security group, the dynamic security group is created in NSX Manager during the import.

The firewall configuration is imported, and the preexisting rule is overwritten.

Load Firewall Configuration

You can load an autosaved or imported firewall configuration. If your current configuration contains rules managed by Service Composer, these are overridden after the import.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > Firewall**.

2 Ensure that you are in the **General** tab to load an L3 firewall configuration. Click the **Ethernet** tab to load an L2 firewall configuration.

3 Click the **Load configuration** ( ) icon.

4 Select the configuration to load and click **OK**.

The current configuration is replaced by the selected configuration.

What to do next

If Service Composer rules in your configuration were overridden by the loaded configuration, click **Actions > Synchronize Firewall Rules** in the Security Policies tab within Service Composer.

Excluding Virtual Machines from Firewall Protection

You can exclude a set of virtual machines from firewall protection.

NSX Manager and Edge virtual machines are automatically excluded from firewall protection. In addition, VMware recommends that you place the following service virtual machines in the Exclusion List to allow traffic to flow freely.

- vCenter Server. It can be moved into a cluster that is protected by Firewall, but it must already exist in the exclusion list to avoid connectivity issues.
- Partner service virtual machines.
- Virtual machines that require promiscuous mode. If these virtual machines are protected by Firewall, their performance may be adversely affected.

Procedure

1 In the vSphere Web Client, click **Networking & Security**.

2 In **Networking & Security Inventory**, click **NSX Managers**.

3 In the **Name** column, click an NSX Manager.

4 Click the **Manage** tab and then click the **Exclusion List** tab.

5 Click the **Add** ( ) icon.

6 Type the name of the virtual machine that you want to exclude and click **Add**.

7 Click **OK**.

If a virtual machine has multiple vNICs, all of them are excluded from protection. If you add vNICs to a virtual machine after it has been added to the Exclusion List, Firewall is automatically deployed on the newly added vNICs. In order to exclude these vNICs from firewall protection, you must remove the virtual machine from the Exclusion List and then add it back to the Exclusion List.

Using SpoofGuard

After synchronizing with the vCenter Server, NSX Manager collects the IP addresses of all vCenter guest virtual machines from VMware Tools on each virtual machine. If a virtual machine has been compromised, the IP address can be spoofed and malicious transmissions can bypass firewall policies.

You create a SpoofGuard policy for specific networks that allows you to authorize the IP addresses reported by VMware Tools and alter them if necessary to prevent spoofing. SpoofGuard inherently trusts the MAC addresses of virtual machines collected from the VMX files and vSphere SDK. Operating separately from Firewall rules, you can use SpoofGuard to block traffic determined to be spoofed.

The SpoofGuard policy monitors and manages the IP addresses reported by your virtual machines in one of the following modes.

Automatically Trust IP Assignments On Their First Use	This mode allows all traffic from your virtual machines to pass while building a table of vNIC-to-IP address assignments. You can review this table at your convenience and make IP address changes. This mode automatically approves all ipv4 and ipv6 address on a vNIC.
Manually Inspect and Approve All IP Assignments Before Use	This mode blocks all traffic until you approve each vNIC-to-IP address assignment.

NOTE SpoofGuard inherently allows DHCP requests regardless of enabled mode. However, if in manual inspection mode, traffic does not pass until the DHCP-assigned IP address has been approved.

SpoofGuard includes a system-generated default policy that applies to port groups and logical networks not covered by the other SpoofGuard policies. A newly added network is automatically added to the default policy until you add the network to an existing policy or create a new policy for it.

Create a SpoofGuard Policy

You can create a SpoofGuard policy to specify the operation mode for specific networks. The system-generated (default) policy applies to port groups and logical switches not covered by existing SpoofGuard policies.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > SpoofGuard**.

2 Click the **Add** icon.

3 Type a name for the policy.

4 Select **Enabled** or **Disabled** to indicate whether the policy is enabled.

5 For **Operation Mode**, select one of the following:

Option	Description
Automatically Trust IP Assignments on Their First Use	Select this option to trust all IP assignments upon initial registration with the NSX Manager.
Manually Inspect and Approve All IP Assignments Before Use	Select this option to require manual approval of all IP addresses. All traffic to and from unapproved IP addresses is blocked.

6 Click **Allow local address as valid address in this namespace** to allow local IP addresses in your setup.

When you power on a virtual machine and it is unable to connect to the DHCP server, a local IP address is assigned to it. This local IP address is considered valid only if the SpoofGuard mode is set to **Allow local address as valid address in this namespace**. Otherwise, the local IP address is ignored.

7 Click **Next**.

8 To specify the scope for the policy, click **Add** and select the networks, distributed port groups, or logical switches that this policy should apply to.

A port group or logical switch can belong to only one SpoofGuard policy.

9 Click **OK** and then click **Finish**.

What to do next

You can edit a policy by clicking the **Edit** icon and delete a policy by clicking the **Delete** icon.

Approve IP Addresses

If you set SpoofGuard to require manual approval of all IP address assignments, you must approve IP address assignments to allow traffic from those virtual machines to pass.

Procedure

1 In the **SpoofGuard** tab, select a policy.

Policy details are displayed below the policy table.

2 In **View**, click one of the option links.

Option	Description
Active Virtual NICs	List of all validated IP addresses
Active Virtual NICs Since Last Published	List of IP addresses that have been validated since the policy was last updated
Virtual NICs IP Required Approval	IP address changes that require approval before traffic can flow to or from these virtual machines
Virtual NICs with Duplicate IP	IP addresses that are duplicates of an existing assigned IP address within the selected datacenter
Inactive Virtual NICs	List of IP addresses where the current IP address does not match the published IP address
Unpublished Virtual NICs IP	List of virtual machines for which you have edited the IP address assignment but have not yet published

3 Do one of the following.

- To approve a single IP address, click **Approve** next to the IP address.
- To approve multiple IP addresses, select the appropriate vNICs and then click **Approve Detected IP(s)**.

Edit an IP Address

You can edit the IP address assigned to a MAC address to correct the assigned IP address.

NOTE SpoofGuard accepts a unique IP address from virtual machines. However, you can assign an IP address only once. An approved IP address is unique across NSX. Duplicate approved IP addresses are not allowed.

Procedure

1 In the **SpoofGuard** tab, select a policy.

Policy details are displayed below the policy table.

2 In **View**, click one of the option links.

Option	Description
Active Virtual NICs	List of all validated IP addresses
Active Virtual NICs Since Last Published	List of IP addresses that have been validated since the policy was last updated
Virtual NICs IP Required Approval	IP address changes that require approval before traffic can flow to or from these virtual machines
Virtual NICs with Duplicate IP	IP addresses that are duplicates of an existing assigned IP address within the selected datacenter
Inactive Virtual NICs	List of IP addresses where the current IP address does not match the published IP address
Unpublished Virtual NICs IP	List of virtual machines for which you have edited the IP address assignment but have not yet published

3 For the appropriate vNIC, click the **Edit** icon and make appropriate changes.

4 Click **OK**.

Clear an IP Address

You clear an approved IP address assignment from a SpoofGuard policy.

Procedure

1 In the **SpoofGuard** tab, select a policy.

Policy details are displayed below the policy table.

2 In **View**, click one of the option links.

Option	Description
Active Virtual NICs	List of all validated IP addresses
Active Virtual NICs Since Last Published	List of IP addresses that have been validated since the policy was last updated
Virtual NICs IP Required Approval	IP address changes that require approval before traffic can flow to or from these virtual machines
Virtual NICs with Duplicate IP	IP addresses that are duplicates of an existing assigned IP address within the selected datacenter
Inactive Virtual NICs	List of IP addresses where the current IP address does not match the published IP address
Unpublished Virtual NICs IP	List of virtual machines for which you have edited the IP address assignment but have not yet published

3 Do one of the following.

- To clear a single IP address, click **Clear** next to the IP address.
- To clear multiple IP addresses, select the appropriate vNICs and then click **Clear Approved IP(s)**.

View Firewall CPU and Memory Threshold Events

When a cluster is prepared for network virtualization, the Firewall module is installed on all hosts of that cluster. This module allocates three heaps, a module heap for module parameters; a rule heap for rules, containers, and filters; and a state heap for traffic flows. Heap size allocation is determined by the available host physical memory. Depending on the number of rules, container sets, and the connections, the heap size may grow or shrink over time. The Firewall module running in the hypervisor also uses the host CPUs for packet processing.

Knowing the host resource utilization at any given time can help you in better organizing your server utilization and network designs.

The default CPU threshold is 100, and the memory threshold is 100. You can modify the default threshold values through REST API calls. The Firewall module generates system events when the memory and CPU usage crosses the thresholds. For information on configuring default threshold values, see Working with Memory and CPU Thresholds in the *NSX API Guide*.

Procedure

1 In the vSphere Web Client, click **Networking & Security** and then click **NSX Managers**.

2 In the **Name** column, click the IP address of the appropriate NSX Manager.

3 Click the **Monitor** tab and then click **System Events**.

Firewall Logs

Firewall generates and stores three types of logs:

- Rules message logs include all access decisions such as permitted or denied traffic for each rule if logging was enabled for that rule. These are stored on each host in `/var/log/vmkernel.log`.
- Audit logs include administration logs and Distributed Firewall configuration changes. These are stored in `/home/secureall/secureall/logs/vsm.log`.
- System event logs include Distributed Firewall configuration applied, filter created, deleted, or failed, and virtual machines added to security groups, etc. These are stored in `/home/secureall/secureall/logs/vsm.log`.

For more information, see Chapter 14, "Operations and Management," on page 157.

Working with Local Rules

You can navigate to an NSX Edge to see the rules that apply to it. These are referred to as local rules.

Firewall rules applied to a Logical Router only protect control plane traffic to and from the Logical Router control virtual machine. They do not enforce any data plane protection. To protect data plane traffic, create Logical Firewall rules for East-West protection or rules at the NSX Edge Services Gateway level for North-South protection.

Rules created on the Firewall user interface applicable to this NSX Edge are displayed in a read-only mode. Rules are displayed and enforced in the following order:

1 User-defined rules from the Firewall user interface (Read Only).

2 Auto-plumbed rules (rules that enable control traffic to flow for Edge services).

3 User-defined rules on NSX Edge Firewall user interface.

4 Default rule.

Edit the Default Local Rule

Default firewall settings apply to traffic that does not match any of the user-defined firewall rules. The default Edge firewall policy blocks all incoming traffic. You can change the default action and logging settings.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.

2 Double-click an NSX Edge.

3 Click the **Manage** tab and then click **Firewall**.

4 Select the **Default Rule**, which is the last rule in the firewall table.

5 Point to the **Action** cell of the new rule and click  .

   a Click **Accept** to allow traffic from or to the specified source and destination.

   b Click **Log** to log all sessions matching this rule.

   Enabling logging can affect performance.

   c Type comments if required.

   d Click **OK**.

6 Click **Publish Changes**.

Add a Local Rule

The Edge Firewall tab displays rules created on the centralized Firewall tab in a read-only mode. Any rules that you add here are not displayed on the centralized Firewall tab.

You can add multiple NSX Edge interfaces and/or IP address groups as the source and destination for firewall rules.

Figure 5-1. Firewall rule for traffic to flow from an NSX Edge interface to an HTTP server

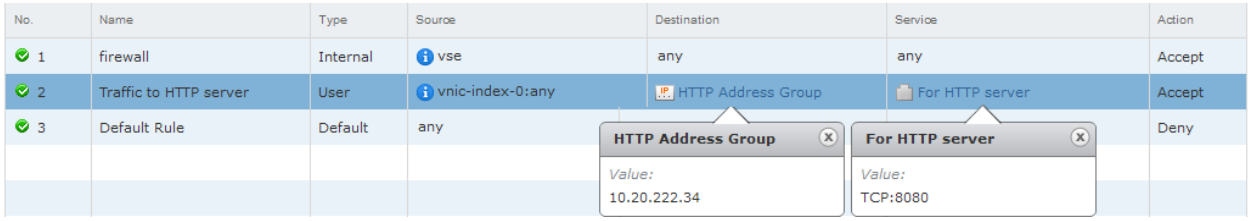
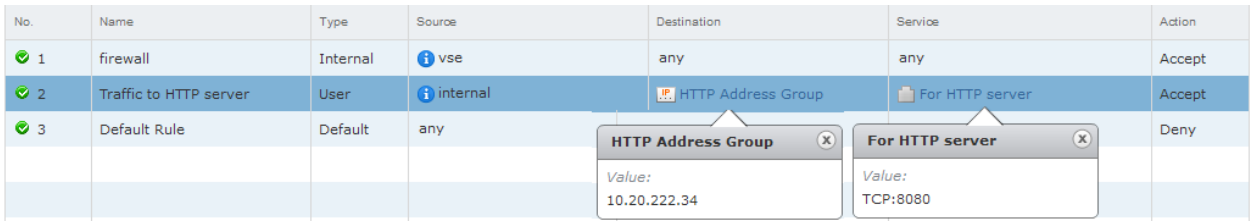
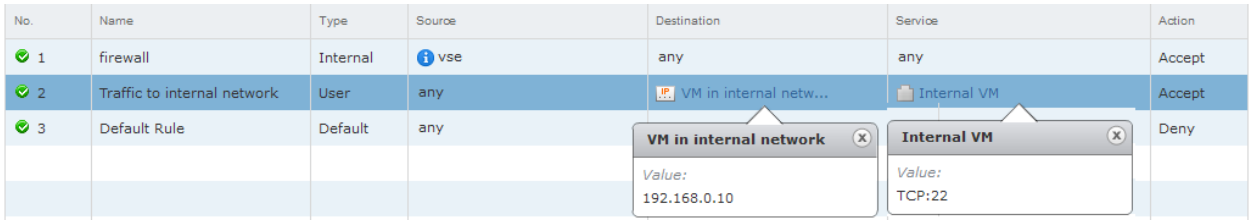


Figure 5-2. Firewall rule for traffic to flow from all internal interfaces (subnets on portgroups connected to internal interfaces) of a NSX Edge to an HTTP Server



NOTE If you select **internal** as the source, the rule is automatically updated when you configure additional internal interfaces.

Figure 5-3. Firewall rule for traffic to allow SSH into a m/c in internal network



Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.

2 Double-click an NSX Edge.

3 Click the **Manage** tab and then click the **Firewall** tab.

4 Do one of the following.

Option	Description
To add a rule at a specific place in the firewall table	a Select a rule. b In the No. column, click and select **Add Above** or **Add Below**. A new any any allow rule is added below the selected rule. If the system defined rule is the only rule in the firewall table, the new rule is added above the default rule.
To add a rule by copying a rule	a Select a rule. b Click the Copy ( ) icon. c Select a rule. d In the No. column, click and select **Paste Above** or **Paste Below**.
To add a rule anywhere in the firewall table	a Click the **Add** ( ) icon. A new any any allow rule is added below the selected rule. If the system defined rule is the only rule in the firewall table, the new rule is added above the default rule.

The new rule is enabled by default.

5 Point to the **Name** cell of the new rule and click .

6 Type a name for the new rule.

7 Point to the **Source** cell of the new rule and click or .

If you clicked , type an IP address.

a Select an object from the drop-down and then make the appropriate selections.

If you select **vNIC Group** and then select **vse**, the rule applies to traffic generated by the NSX Edge. If you select **internal** or **external**, the rule applies to traffic coming from any internal or uplink interface of the selected NSX Edge instance. The rule is automatically updated when you configure additional interfaces.

If you select **IP Sets**, you can create a new IP address group. After you create the new group, it is automatically added to the source column. For information on creating an IP Set, see "Create an IP Address Group," on page 149.

b Click **OK**.

8 Point to the **Destination** cell of the new rule and click or .

a Select an object from the drop-down and then make the appropriate selections.

If you select **vNIC Group** and then select **vse**, the rule applies to traffic generated by the NSX Edge. If you select **internal** or **external**, the rule applies to traffic going to any internal or uplink interface of the selected NSX Edge instance. The rule is automatically updated when you configure additional interfaces.

If you select **IP Sets**, you can create a new IP address group. After you create the new group, it is automatically added to the source column. For information on creating an IP Set, see "Create an IP Address Group," on page 149.

b Click **OK**.

9 Point to the **Service** cell of the new rule and click or .

- If you clicked , select a service. To create a new service or service group, click **New**. After you create the new service, it is automatically added to the Service column. For more information on creating a new service, see "Create a Service," on page 154.
- If you clicked , select a protocol. You can specify the source port by clicking the arrow next to Advanced options. VMware recommends that you avoid specifying the source port from release 5.1 and later. Instead, you can create a service for a protocol-port combination.

NOTE NSX Edge only supports services defined with L3 protocols.

10 Point to the **Action** cell of the new rule and click . Make appropriate selections as described in the table below and click **OK**.

Action selected	Results in
Allow	Allows traffic from or to the specified source and destination.
Block	Blocks traffic from or to the specified source and destination.
Reject	Sends reject message for unaccepted packets. RST packets are sent for TCP packets. ICMP unreachable (administratively restricted) packets are sent for other packets.
Log	Logs all sessions matching this rule. Enabling logging can affect performance.
Do not log	Does not log sessions.
Comments	Type comments if required.
Advanced options > Match on Translated	Applies the rule to the translated IP address and services for a NAT rule
Enable Rule Direction	Indicates whether the rule is incoming or outgoing. VMware does not recommend specifying the direction for firewall rules.

11 Click **Publish Changes** to push the new rule to the NSX Edge instance.

What to do next

- Disable a rule by clicking next to the rule number in the **No.** column.
- Hide generated rules or pre rules (rules added on the centralized Firewall tab) by clicking **Hide Generated rules** or **Hide Pre rules**.

- Display additional columns in the rule table by clicking  and selecting the appropriate columns.

Column Name	Information Displayed
Rule Tag	Unique system generated ID for each rule
Log	Traffic for this rule is being logged or not
Stats	Clicking  shows the traffic affected by this rule (number of sessions, traffic packets, and size)
Comments	Comments for the rule

- Search for rules by typing text in the Search field.

Edit a Local Rule

You can edit only the user-defined firewall rules that were added in the Edge Firewall tab. Rules added on the centralized Firewall tab are not editable on the Edge Firewall tab.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.

2 Double-click an NSX Edge.

3 Click the **Monitor** tab and then click the **Firewall** tab.

4 Select the rule to edit

NOTE You cannot change an auto-generated rule or the default rule.

5 Make the desired changes and click **OK**.

6 Click **Publish Changes**.

Change the Priority of a Local Rule

You can change the order of user-defined firewall rules that were added in the Edge Firewall tab to customize traffic flowing through the NSX Edge. For example, suppose you have a rule to allow load balancer traffic. You can now add a rule to deny load balancer traffic from a specific IP address group, and position this rule above the LB allow traffic rule.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.

2 Double-click an NSX Edge.

3 Click the **Monitor** tab and then click the **Firewall** tab.

4 Select the rule for which you want to change the priority.

NOTE You cannot change the priority of auto-generated rules or the default rule.

5 Click the **Move Up** () or **Move Down** () icon.

6 Click **OK**.

7 Click **Publish Changes**.

Delete a Local Rule

You can delete a user-defined firewall rule that was added in the NSX Edge Firewall tab. Rules added on the centralized Firewall tab cannot be deleted here.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.

2 Double-click an NSX Edge.

3 Click the **Monitor** tab and then click the **Firewall** tab.

4 Select the rule to delete.

NOTE You cannot delete an auto-generated rule or the default rule.

5 Click the **Delete** ( ) icon.

Managing NAT Rules

NSX Edge provides network address translation (NAT) service to assign a public address to a computer or group of computers in a private network. Using this technology limits the number of public IP addresses that an organization or company must use, for economy and security purposes. You must configure NAT rules to provide access to services running on privately addressed virtual machines.

The NAT service configuration is separated into source NAT (SNAT) and destination NAT (DNAT) rules.

Add an SNAT Rule

You can create a source NAT (SNAT) rule to change the source IP address from a public to private IP address or the reverse.

Prerequisites

The translated (public) IP address must have been added to the NSX Edge interface on which you want to add the rule.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.

2 Double-click an NSX Edge.

3 Click the **Manage** tab and then click the **NAT** tab.

4 Click the **Add** ( ) icon and select **Add SNAT Rule**.

5 Select the interface on which to add the rule.

6 Type the original source IP address in one of the following formats.

Format	Example
IP address	192.0.2.0
IP address range	192.0.2.0-192.0.2.24
IP address/subnet	192.0.2.0/24
any	

7 Type the translated (public) source IP address in one of the following formats.

Format	Example
IP address	192.0.2.0
IP address range	192.0.2.0-192.0.2.24
IP address/subnet	192.0.2.0/24
any	

8 Select **Enabled** to enable the rule.

9 Click **Enable logging** to log the address translation.

10 Click **OK** to add the rule.

11 Click **Publish Changes**.

Add a DNAT Rule

You can create a destination NAT (DNAT) rule to change the destination IP address from a public to private IP address or the reverse.

Prerequisites

The original (public) IP address must have been added to the NSX Edge interface on which you want to add the rule.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **NAT** tab.

5 Click the **Add** ( ) icon and select **Add DNAT Rule**.

6 Select the interface on which to apply the DNAT rule.

7 Type the original (public) IP address in one of the following formats.

Format	Example
IP address	192.0.2.0
IP address range	192.0.2.0 -192.0.2.24
IP address/subnet	192.0.2.0 /24
any	

8 Type the protocol.

9 Type the original port or port range.

Format	Example
Port number	80
Port range	80-85
any	

10 Type the translated IP address in one of the following formats.

Format	Example
IP address	192.0.2.0
IP address range	192.0.2.0 -192.0.2.24
IP address/subnet	192.0.2.0 /24
any	

11 Type the translated port or port range.

Format	Example
Port number	80
Port range	80-85
any	

12 Select **Enabled** to enable the rule.

13 Select **Enable logging** to log the address translation.

14 Click **Add** to save the rule.

Virtual Private Networks (VPN)s

6

NSX Edge supports several types of VPNs. SSL VPN-Plus allows remote users to access private corporate applications. IPSec VPN offers site-to-site connectivity between an NSX Edge instance and remote sites. L2 VPN allows you to extend your datacenter by allowing virtual machines to retain network connectivity across geographical boundaries.

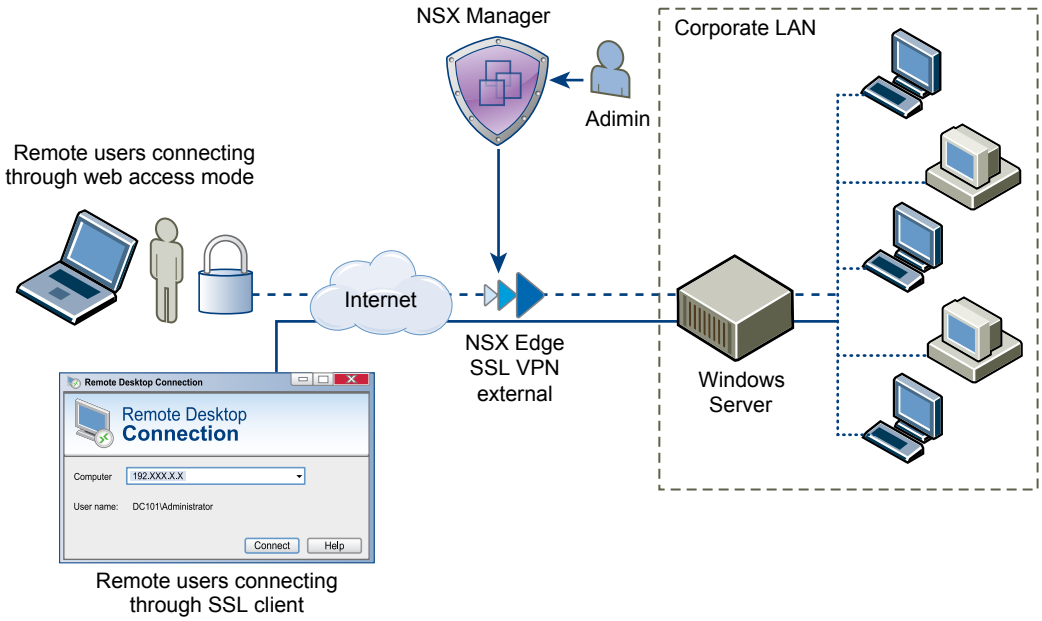
You must have a working NSX Edge instance before you can use VPN. For information on setting up NSX Edge, see "NSX Edge Operations," on page 166.

This chapter includes the following topics:

- "SSL VPN-Plus Overview," on page 65
- "IPSec VPN Overview," on page 85
- "L2 VPN Overview," on page 89

SSL VPN-Plus Overview

With SSL VPN-Plus, remote users can connect securely to private networks behind a NSX Edge gateway. Remote users can access servers and applications in the private networks.



Configure Network Access SSL VPN-Plus

In network access mode, a remote user can access private networks after downloading and installing an SSL client.

Prerequisites

The SSL VPN gateway requires port 443 to be accessible from external networks and the SSL VPN client requires the NSX Edge gateway IP and port 443 to be reachable from client system.

Procedure

1 Add SSL VPN-Plus Server Settings on page 66

You must add SSL VPN server settings to enable SSL on a NSX Edge interface.

2 Add an IP Pool on page 67

The remote user is assigned a virtual IP address from the IP pool that you add.

3 Add a Private Network on page 67

Add the network that you want the remote user to be able to access.

4 Add Authentication on page 68

Instead of a local user, you can add an external authentication server (AD, LDAP, Radius, or RSA) which is bound to the SSL gateway. All users with accounts on the bound authentication server will be authenticated.

5 Add Installation Package on page 71

Create an installation package of the SSL VPN-Plus client for the remote user.

6 Add a User on page 72

Add a remote user to the local database.

7 Enable the SSL VPN-Plus Service on page 72

After configuring the SSL VPN-Plus service, enable the service for remote users to begin accessing private networks.

8 Add a Script on page 73

You can add multiple login or logoff scripts. For example, you can bind a login script for starting Internet Explorer with gmail.com. When the remote user logs in to the SSL client, Internet Explorer opens up gmail.com.

9 Install SSL Client on Remote Site on page 73

This section describes the procedure a remote user can follow on his/her desktop after SSL VPN-Plus is configured. Windows, MAC, and Linux desktops are supported.

Add SSL VPN-Plus Server Settings

You must add SSL VPN server settings to enable SSL on a NSX Edge interface.

Procedure

1 In the **SSL VPN-Plus** tab, **Server Settings** from the left panel.

2 Click **Change.**

3 Select the IPv4 or IPv6 address.

4 Edit the port number if required. This port number is required to configure the installation package.

5 Select the encryption method.

6 (Optional) From the Server Certificates table, select the server certificate that you want to add.

7 Click **OK.**

Add an IP Pool

The remote user is assigned a virtual IP address from the IP pool that you add.

Procedure

1 In the **SSL Vpn-Plus** tab, select **IP Pools** from the left panel.

2 Click the **Add** ( ) icon.

3 Type the begin and end IP address for the IP pool.

4 Type the netmask of the IP pool.

5 Type the IP address which is to add the routing interface in the NSX Edge gateway.

6 (Optional) Type a description for the IP pool.

7 Select whether to enable or disable the IP pool.

8 (Optional) In the **Advanced** panel, type the DNS name.

9 (Optional) Type the secondary DNS name.

10 Type the connection-specific DNS suffix for domain based host name resolution.

11 Type the WINS server address.

12 Click **OK**.

Add a Private Network

Add the network that you want the remote user to be able to access.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Private Networks** from the left panel.

2 Click the **Add** ( ) icon

3 Type the private network IP address.

4 Type the netmask of the private network.

5 (Optional) Type a description for the network.

6 Specify whether you want to send private network and internet traffic over the SSL VPN-Plus enabled NSX Edge or directly to the private server by bypassing the NSX Edge.

7 If you selected **Send traffic over the tunnel**, select **Enable TCP Optimization** to optimize the internet speed.

Conventional full-access SSL VPNs tunnel sends TCP/IP data in a second TCP/IP stack for encryption over the internet. This results in application layer data being encapsulated twice in two separate TCP streams. When packet loss occurs (which happens even under optimal internet conditions), a performance degradation effect called TCP-over-TCP meltdown occurs. In essence, two TCP instruments are correcting a single packet of IP data, undermining network throughput and causing connection timeouts. TCP Optimization eliminates this TCP-over-TCP problem, ensuring optimal performance.

8 Type the port numbers that you want to open for the remote user to access the corporate internal servers/machines like 3389 for RDP, 20/21 for FTP, and 80 for http. If you want to give unrestricted access to the user, you can leave the **Ports** field blank.

9 Specify whether you want to enable or disable the private network.

10 Click **OK**.

What to do next

Add a corresponding firewall rule to allow the private network traffic.

Add Authentication

Instead of a local user, you can add an external authentication server (AD, LDAP, Radius, or RSA) which is bound to the SSL gateway. All users with accounts on the bound authentication server will be authenticated.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Authentication** from the left panel.

2 Click the **Add** ( ) icon.

3 Select the type of authentication server.

4 Depending on the type of authentication server you selected, complete the following fields.

- AD authentication server

Table 6-1. AD Authentication Server Options

Option	Description
Enable SSL	Enabling SSL establishes an encrypted link between a web server and a browser.
IP Address	IP address of the authentication server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Search base	Part of the external directory tree to search. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.
Bind DN	User on the external AD server permitted to search the AD directory within the defined search base. Most of the time, the bind DN is permitted to search the entire directory. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating AD users. When the DN is returned, the DN and password are used to authenticate the AD user.
Bind Password	Password to authenticate the AD user.
Retype Bind Password	Retype the password.
Login Attribute Name	Name against which the user ID entered by the remote user is matched with. For Active Directory, the login attribute name is **`sAMAccountName`**.
Search Filter	Filter values by which the search is to be limited. The search filter format is *attribute operator value*.

Table 6-1. AD Authentication Server Options (Continued)

Option	Description
Use this server for secondary authentication	If selected, this AD server is used as the second level of authentication.
Terminate Session if authenticati on fails	When selected, the session is ended if authentication fails.

- LDAP authentication server

Table 6-2. LDAP Authentication Server Options

Option	Description
Enable SSL	Enabling SSL establishes an encrypted link between a web server and a browser.
IP Address	IP address of the external server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Search base	Part of the external directory tree to search. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.
Bind DN	User on the external server permitted to search the AD directory within the defined search base. Most of the time, the bind DN is permitted to search the entire directory. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating AD users. When the DN is returned, the DN and password are used to authenticate the AD user.
Bind Password	Password to authenticate the AD user.
Retype Bind Password	Retype the password.
Login Attribute Name	Name against which the user ID entered by the remote user is matched with. For Active Directory, the login attribute name is **sAMAccountName**.
Search Filter	Filter values by which the search is to be limited. The search filter format is *attribute operator value*.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
Terminate Session if authentication fails	When selected, the session is ended if authentication fails.

- RADIUS authentication server

Table 6-3. RADIUS authentication server options

Option	Description
IP Address	IP address of the external server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Secret	Shared secret specified while adding the authentication agent in the RSA security console.
Retype secret	Retype the shared secret.

Table 6-3. RADIUS authentication server options (Continued)

Option	Description
NAS IP Address	IP address to be configured and used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets.
Retry Count	Number of times the RADIUS server is to be contacted if it does not respond before the authentication fails.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
`Terminate Session if authenticatio n fails`	When selected, the session is ended if authentication fails.

- RSA-ACE authentication server

Table 6-4. RSA-ACE authentication server options

Option	Description
Timeout	Period in seconds within which the AD server must respond.
Configuration File	Click **Browse** to select the `sdconf.rec` file that you downloaded from the RSA Authentication Manager.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Source IP Address	IP address of the NSX Edge interface through which the RSA server is accessible.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
`Terminate Session if authenticatio n fails`	When selected, the session is ended if authentication fails.

- Local authentication server

Table 6-5. Local authentication server options

Option	Description
Enable password policy	If selected, defines a password policy. Specify the required values.
Enable password policy	If selected, defines an account lockout policy. Specify the required values. 1 In Retry Count, type the number of times a remote user can try to access his or her account after entering an incorrect password. 2 In Retry Duration, type the time period in which the remote user's account gets locked on unsuccessful login attempts. For example, if you specify Retry Count as 5 and Retry Duration as 1 minute, the remote user's account will be locked if he makes 5 unsuccessful login attempts within 1 minute. 3 In Lockout Duration, type the time period for which the user account remains locked. After this time, the account is automatically unlocked.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.

Table 6-5. Local authentication server options (Continued)

Option	Description
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
Terminate Session if authentication fails	When selected, the session is ended if authentication fails.

Add Installation Package

Create an installation package of the SSL VPN-Plus client for the remote user.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Installation Package** from the left panel.

2 Click the **Add** ( ) icon.

3 Type a profile name for the installation package.

4 In **Gateway**, type the IP address or FQDN of the public interface of NSX Edge.

This IP address or FQDN is binded to the SSL client. When the client is installed, this IP address or FQDN is displayed on the SSL client.

5 Type the port number that you specified in the server settings for SSL VPN-Plus. See "Add SSL VPN-Plus Server Settings," on page 66.

6 (Optional) To bind additional NSX Edge uplink interfaces to the SSL client,

a Click the **Add** ( ) icon.

b Type the IP address and port number.

c Click **OK**.

7 The installation package is created for Windows operating system by default. Select Linux or Mac to create an installation package for Linux or Mac operating systems as well.

8 (Optional) Enter a description for the installation package.

9 Select **Enable** to display the installation package on the Installation Package page.

10 Select the following options as appropriate.

Option	Description
Start client on logon	The SSL VPN client is started when the remote user logs on to his system.
Allow remember password	Enables the option.
Enable silent mode installation	Hides installation commands from remote user.
Hide SSL client network adapter	Hides the VMware SSL VPN-Plus Adapter, which is installed on the remote user's computer along with the SSL VPN installation package.
Hide client system tray icon	Hides the SSL VPN tray icon which indicates whether the VPN connection is active or not.
Create desktop icon	Creates an icon to invoke the SSL client on the user's desktop.
Enable silent mode operation	Hides the pop-up that indicates that installation is complete.
Server security certificate validation	The SSL VPN client validates the SSL VPN server certificate before establishing the secure connection.

11 Click **OK.**

Add a User

Add a remote user to the local database.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Users** from the left panel.

2 Click the **Add** ( ) icon.

3 Type the user ID.

4 Type the password.

5 Retype the password.

6 (Optional) Type the first and last name of the user.

7 (Optional) Type a description for the user.

8 In Password Details, select **Password never expires** to always keep the same password for the user.

9 Select **Allow change password** to let the user change the password.

10 Select **Change password on next login** if you want the user to change the password the next time he logs in.

11 Set the user status.

12 Click **OK**.

Enable the SSL VPN-Plus Service

After configuring the SSL VPN-Plus service, enable the service for remote users to begin accessing private networks.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Dashboard** from the left panel.

2 Click the Enable icon.

The dashboard displays the status of the service, number of active SSL VPN sessions, and session statistics and data flow details. Click **Details** next to Number of Active Sessions to view information about the concurrent connections to private networks behind the NSX Edge gateway.

What to do next

1 Add an SNAT rule to translate the IP address of the NSX Edge appliance to the VPN Edge IP address.

2 Using a web browser, navigate to the IP address of the NSX Edge interface by typing `https//NSXEdgeIPAddress`.

3 Login using the user name and password that you created in the "Add a User," on page 72 section and download the installation package.

4 Enable port forwarding on your router for the port number used in "Add SSL VPN-Plus Server Settings," on page 66.

5 Launch the VN client, select your VPN server, and login. You can now navigate to the services on your network. SSL VPN-Plus gateway logs are sent to the syslog server configured on the NSX Edge appliance. SSL VPN-Plus client logs are stored in the following directory on the remote user's computer: `%PROGRAMFILES%/VMWARE/SSLVPN Client/`.

Add a Script

You can add multiple login or logoff scripts. For example, you can bind a login script for starting Internet Explorer with gmail.com. When the remote user logs in to the SSL client, Internet Explorer opens up gmail.com.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Login/Logoff Scripts** from the left panel.

2 Click the **Add** ( ) icon.

3 In **Script**, click **Browse** and select the script you want to bind to the NSX Edge gateway.

4 Select the **Type** of script.

Option	Description
Login	Performs the script action when remote user logs in to SSL VPN.
Logoff	Performs the script action when remote user logs out of SSL VPN.
Both	Performs the script action both when remote user logs in and logs out of SSL VPN.

5 Type a description for the script.

6 Select **Enabled** to enable the script.

7 Click **OK**.

Install SSL Client on Remote Site

This section describes the procedure a remote user can follow on his/her desktop after SSL VPN-Plus is configured. Windows, MAC, and Linux desktops are supported.

Procedure

1 On the client site, the remote user can type (`https://`*ExternalEdgeInterfaceIP*`/sslvpn-plus/`) in a browser window where *ExternalEdgeInterfaceIP* is the IP address of the Edge external interface where you enabled SSL VPN-Plus.

2 Login to the portal using the user name and password created in the Users section.

3 Click SSL client.

The SSL client is downloaded.

4 Login to the SSL client with the credentials specified in the Users section.

The remote user can now access the private network.

Configure Web Access SSL VPN-Plus

In web access mode, a remote user can access private networks without a hardware or software SSL client.

Procedure

1 Create a Web Resource on page 74

Add a server that the remote user can connect to via a web browser.

2 Add a User on page 74

Add a remote user to the local database.

3 Add Authentication on page 75

Instead of a local user, you can add an external authentication server (AD, LDAP, Radius, or RSA) which is bound to the SSL gateway. All users with accounts on the bound authentication server will be authenticated.

4 Add SSL VPN-Plus Server Settings on page 78

You must add SSL VPN server settings to enable SSL on a NSX Edge interface.

5 Enable the SSL VPN-Plus Service on page 78

After configuring the SSL VPN-Plus service, enable the service for remote users to begin accessing private networks.

6 Add a Script on page 79

You can add multiple login or logoff scripts. For example, you can bind a login script for starting Internet Explorer with gmail.com. When the remote user logs in to the SSL client, Internet Explorer opens up gmail.com.

Create a Web Resource

Add a server that the remote user can connect to via a web browser.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click the **SSL VPN-Plus** tab.

5 Select **Web Resource** from the left panel.

6 Click the **Add** ( ) icon.

7 Type a name for the web resource.

8 Type the URL of the web resource that you want the remote user to access.

9 Depending on whether the remote user wants to read from or write to the web resource, select the **HTTPMethod** and type the GET or POST call.

10 Type the description for the web resource. This description is displayed on the web portal when the remote user accesses the web resource.

11 Select **Enable** to enable the web resource. The web resource must be enabled for the remote user to access it.

Add a User

Add a remote user to the local database.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Users** from the left panel.

2 Click the **Add** ( ) icon.

3 Type the user ID.

4 Type the password.

5 Retype the password.

6 (Optional) Type the first and last name of the user.

7 (Optional) Type a description for the user.

8 In Password Details, select **Password never expires** to always keep the same password for the user.

9 Select **Allow change password** to let the user change the password.

10 Select **Change password on next login** if you want the user to change the password the next time he logs in.

11 Set the user status.

12 Click **OK**.

Add Authentication

Instead of a local user, you can add an external authentication server (AD, LDAP, Radius, or RSA) which is bound to the SSL gateway. All users with accounts on the bound authentication server will be authenticated.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Authentication** from the left panel.

2 Click the **Add** ( ) icon.

3 Select the type of authentication server.

4 Depending on the type of authentication server you selected, complete the following fields.

- AD authentication server

Table 6-6. AD Authentication Server Options

Option	Description
Enable SSL	Enabling SSL establishes an encrypted link between a web server and a browser.
IP Address	IP address of the authentication server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Search base	Part of the external directory tree to search. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.
Bind DN	User on the external AD server permitted to search the AD directory within the defined search base. Most of the time, the bind DN is permitted to search the entire directory. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating AD users. When the DN is returned, the DN and password are used to authenticate the AD user.
Bind Password	Password to authenticate the AD user.
Retype Bind Password	Retype the password.
Login Attribute Name	Name against which the user ID entered by the remote user is matched with. For Active Directory, the login attribute name is **`sAMAccountName`**.
Search Filter	Filter values by which the search is to be limited. The search filter format is *attribute operator value*.

Table 6-6. AD Authentication Server Options (Continued)

Option	Description
Use this server for secondary authentication	If selected, this AD server is used as the second level of authentication.
Terminate Session if authenticati on fails	When selected, the session is ended if authentication fails.

- LDAP authentication server

Table 6-7. LDAP Authentication Server Options

Option	Description
Enable SSL	Enabling SSL establishes an encrypted link between a web server and a browser.
IP Address	IP address of the external server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Search base	Part of the external directory tree to search. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.
Bind DN	User on the external server permitted to search the AD directory within the defined search base. Most of the time, the bind DN is permitted to search the entire directory. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating AD users. When the DN is returned, the DN and password are used to authenticate the AD user.
Bind Password	Password to authenticate the AD user.
Retype Bind Password	Retype the password.
Login Attribute Name	Name against which the user ID entered by the remote user is matched with. For Active Directory, the login attribute name is **sAMAccountName**.
Search Filter	Filter values by which the search is to be limited. The search filter format is *attribute operator value*.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
Terminate Session if authentication fails	When selected, the session is ended if authentication fails.

- RADIUS authentication server

Table 6-8. RADIUS authentication server options

Option	Description
IP Address	IP address of the external server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Secret	Shared secret specified while adding the authentication agent in the RSA security console.
Retype secret	Retype the shared secret.

Table 6-8. RADIUS authentication server options (Continued)

Option	Description
NAS IP Address	IP address to be configured and used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets.
Retry Count	Number of times the RADIUS server is to be contacted if it does not respond before the authentication fails.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
`Terminate Session if authenticatio n fails`	When selected, the session is ended if authentication fails.

- RSA-ACE authentication server

Table 6-9. RSA-ACE authentication server options

Option	Description
Timeout	Period in seconds within which the AD server must respond.
Configuration File	Click **Browse** to select the `sdconf.rec` file that you downloaded from the RSA Authentication Manager.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Source IP Address	IP address of the NSX Edge interface through which the RSA server is accessible.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
`Terminate Session if authenticatio n fails`	When selected, the session is ended if authentication fails.

- Local authentication server

Table 6-10. Local authentication server options

Option	Description
Enable password policy	If selected, defines a password policy. Specify the required values.
Enable password policy	If selected, defines an account lockout policy. Specify the required values. 1 In Retry Count, type the number of times a remote user can try to access his or her account after entering an incorrect password. 2 In Retry Duration, type the time period in which the remote user's account gets locked on unsuccessful login attempts. For example, if you specify Retry Count as 5 and Retry Duration as 1 minute, the remote user's account will be locked if he makes 5 unsuccessful login attempts within 1 minute. 3 In Lockout Duration, type the time period for which the user account remains locked. After this time, the account is automatically unlocked.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.

Table 6-10. Local authentication server options (Continued)

Option	Description
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
Terminate Session if authentication fails	When selected, the session is ended if authentication fails.

Add SSL VPN-Plus Server Settings

You must add SSL VPN server settings to enable SSL on a NSX Edge interface.

Procedure

1 In the **SSL VPN-Plus** tab, **Server Settings** from the left panel.

2 Click **Change.**

3 Select the IPv4 or IPv6 address.

4 Edit the port number if required. This port number is required to configure the installation package.

5 Select the encryption method.

6 (Optional) From the Server Certificates table, select the server certificate that you want to add.

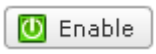
7 Click **OK.**

Enable the SSL VPN-Plus Service

After configuring the SSL VPN-Plus service, enable the service for remote users to begin accessing private networks.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Dashboard** from the left panel.

2 Click the 

icon.

The dashboard displays the status of the service, number of active SSL VPN sessions, and session statistics and data flow details. Click **Details** next to Number of Active Sessions to view information about the concurrent connections to private networks behind the NSX Edge gateway.

What to do next

1 Add an SNAT rule to translate the IP address of the NSX Edge appliance to the VPN Edge IP address.

2 Using a web browser, navigate to the IP address of the NSX Edge interface by typing **`https//NSXEdgeIPAddress`**.

3 Login using the user name and password that you created in the "Add a User," on page 72 section and download the installation package.

4 Enable port forwarding on your router for the port number used in "Add SSL VPN-Plus Server Settings," on page 66.

5 Launch the VN client, select your VPN server, and login. You can now navigate to the services on your network. SSL VPN-Plus gateway logs are sent to the syslog server configured on the NSX Edge appliance. SSL VPN-Plus client logs are stored in the following directory on the remote user's computer: `%PROGRAMFILES%/VMWARE/SSLVPN Client/`.

Add a Script

You can add multiple login or logoff scripts. For example, you can bind a login script for starting Internet Explorer with gmail.com. When the remote user logs in to the SSL client, Internet Explorer opens up gmail.com.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Login/Logoff Scripts** from the left panel.

2 Click the **Add** () icon.

3 In **Script**, click **Browse** and select the script you want to bind to the NSX Edge gateway.

4 Select the **Type** of script.

Option	Description
Login	Performs the script action when remote user logs in to SSL VPN.
Logoff	Performs the script action when remote user logs out of SSL VPN.
Both	Performs the script action both when remote user logs in and logs out of SSL VPN.

5 Type a description for the script.

6 Select **Enabled** to enable the script.

7 Click **OK**.

SSL VPN-Plus Logs

SSL VPN-Plus gateway logs are sent to the syslog server configured on the NSX Edge appliance. SSL VPN-Plus client logs are stored in the following directory on the remote user's computer: `%PROGRAMFILES %/VMWARE/SSL VPN Client/`.

Edit Client Configuration

You can change the way the SSL VPN client tunnel responds when the remote user logs in to SSL VPN.

Procedure

1 In the **SSL VPN-Plus** tab, select **Client Configuration** from the left panel.

2 Select the **Tunneling Mode**.

In split tunnel mode, only the VPN flows through the NSX Edge gateway. In full tunnel, the NSX Edge gateway becomes the remote user's default gateway and all traffic (VPN, local, and internet) flows through this gateway.

3 If you selected the full tunnel mode:

a Select **Exclude local subnets** to exclude local traffic from flowing through the VPN tunnel.

b Type the IP address for the default gateway of the remote user's system.

4 Select **Enable auto reconnect** if you would like the remote user to automatically reconnect to the SSL VPN client after getting disconnected.

5 Select **Client upgrade notification** for the remote user to get a notification when an upgrade for the client is available. The remote user can then choose to install the upgrade.

6 Click **OK**.

Edit General Settings

You can edit the default VPN settings.

Procedure

1 In the **SSL VPN-Plus** tab, select **General Settings** from the left panel.

2 Make required selections.

Select	To
Prevent multiple logon using same username	Allow a remote user to login only once with a username.
Enable compression	Enable TCP based intelligent data compression and improve data transfer speed.
Enable logging	Maintain a log of the traffic passing through the SSL VPN gateway.
Force virtual keyboard	Allow remote users to enter web or client login information only via the virtual keyboard.
Randomize keys of virtual keyboard	Make the virtual keyboard keys random.
Enable forced timeout	Disconnect the remote user after the specified timeout period is over. Type the timeout period in minutes.
Session idle timeout	If there is no activity on the user session for the specified period, end the user session after that period is over.
User notification	Type a message to be displayed to the remote user after he logs in.
Enable public URL access	Allow remote user to access any site which is not configured (and not listed on web portal) by administrator.

3 Click **OK**.

Edit Web Portal Design

You can edit the client banner bound to the SSL VPN client.

Procedure

1 In the **NSX Edges** tab, double-click an NSX Edge.

2 Click the **Monitor** tab and then click the **SSL VPN-Plus** tab.

3 Select **Portal Customization** from the left panel.

4 Type the portal title.

5 Type the remote user's company name.

6 In **Logo**, click **Change** and select the image file for the remote user's logo.

7 In **Colors**, click the color box next to numbered item for which you want to change the color, and select the desired color.

8 If desired, change the client banner.

9 Click **OK**.

Working with IP Pools

You can edit or delete an IP pool.

For information on adding an IP pool, see "Configure Network Access SSL VPN-Plus," on page 66 or "Configure Web Access SSL VPN-Plus," on page 73.

Edit an IP Pool

You can edit an IP pool.

Procedure

1 In the **SSL VPN-Plus** tab, click **IP Pool** in the left panel.

2 Select the IP pool that you want to edit.

3 Click the **Edit** ( ) icon.

The Edit IP Pool dialog box opens.

4 Make the required edits.

5 Click **OK**.

Delete an IP Pool

You can delete an IP pool.

Procedure

1 In the **SSL VPN-Plus** tab, click **IP Pool** in the left panel.

2 Select the IP pool that you want to delete.

3 Click the **Delete** ( ) icon.

The selected IP pool is deleted.

Enable an IP Pool

You can enable an IP pool if you want an IP address from that pool to be assigned to the remote user.

Procedure

1 In the **SSL VPN-Plus** tab, click **IP Pool** in the left panel.

2 Select the IP pool that you want to enable.

3 Click the **Enable** ( ) icon.

Disable an IP Pool

You can disable an IP pool if you do not want the remote user to be assigned an IP address from that pool.

Procedure

1 In the **SSL VPN-Plus** tab, select **IP Pool** from the left panel.

2 Select the IP pool that you want to disable.

3 Click the **Disable** ( ) icon.

Change the Order of an IP Pool

SSL VPN assigns an IP address to a remote user from an IP pool based on its order in the IP pool table.

Procedure

1 In the **SSL VPN-Plus** tab, click **IP Pool** in the left panel.

2 Select the IP pool that you want to change the order for.

3 Click the **Move Up** ( ) or Move Down ( ) icon.

Working with Private Networks

You can edit or delete a private network that a remote user can access.

For information on adding a private network, see "Configure Network Access SSL VPN-Plus," on page 66 or "Configure Web Access SSL VPN-Plus," on page 73.

Delete a Private Network

You can delete a private network

Procedure

1 In the **SSL VPN-Plus** tab, click **Private Networks** in the left panel.

2 Select the network that you want to delete and click the **Delete** ( ) icon.

Enable a Private Network

When you enable a private network, the remote user can access it through SSL VPN-Plus.

Procedure

1 In the **SSL VPN-Plus** tab, click **Private Networks** in the left panel.

2 Click the network that you want to enable.

3 Click the **Enable** icon ( ).

The selected network is enabled.

Disable a Private Network

When you disable a private network, the remote user cannot access it through SSL VPN-Plus.

Procedure

1 In the **SSL VPN-Plus** tab, click **Private Networks** in the left panel.

2 Click the network that you want to disable.

3 Click the **Disable** ( ) icon.

The selected network is disabled.

Change the Sequence of a Private Network

SSL VPN-Plus allows remote users to access private networks in the sequence in which they are displayed on the Private Networks panel.

If you select **Enable TCP Optimization** for a private network, some applications such as FTP in Active mode may not work within that subnet. To add an FTP server configured in Active mode, you must add another private network for that FTP server with TCP Optimization disabled. Also, the active TCP private network must be enabled, and must be placed above the subnet private network.

Procedure

1 In the **SSL VPN-Plus** tab, click **Private Networks** in the left panel.

2 Click the **Change Order** ( ) icon.

3 Select the network that you want to change the order of.

4 Click the **Move Up** ( )or **Move Down** ( ) icon.

5 Click **OK**.

Working with Installation Packages

You can delete or edit an installation package for the SSL client.

For information on creating an installation package, see "Configure Network Access SSL VPN-Plus," on page 66 or "Configure Web Access SSL VPN-Plus," on page 73.

Edit an Installation Package

You can edit an installation package.

Procedure

1 In the **SSL VPN-Plus** tab, click **Installation Package** in the left panel.

2 Select the installation package that you want to edit.

3 Click the Edit ( ) icon.

The Edit Installation Package dialog box opens.

4 Make the required edits.

5 Click **OK**.

Delete an Installation Package

You can delete an installation package.

Procedure

1 In the **SSL VPN-Plus** tab, click **Installation Package** in the left panel.

2 Select the installation package that you want to delete.

3 Click the **Delete** ( ) icon.

Working with Users

You can edit or delete users from the local database.

For information on adding a user, see "Configure Network Access SSL VPN-Plus," on page 66 or "Configure Web Access SSL VPN-Plus," on page 73.

Edit a User

You can edit the details for a user except for the user ID.

Procedure

1 In the **SSL VPN-Plus** tab, click **Users** in the left panel.

2 Click the **Edit** ( ) icon.

3 Make the required edits.

4 Click **OK**.

Delete a User

You can delete a user.

Procedure

1 In the **SSL VPN-Plus** tab, click **Users** in the left panel.

2 **Users**In the **Configure** panel, click **Users**.

3 Select the user that you want to delete and click the **Delete** ( ) icon.

Change the Password for a User

You can change the password for a user.

Procedure

1 In the **SSL VPN-Plus** tab, click **Users** in the left panel.

2 Click the **Change Password** icon.

3 Type and re-type the new password.

4 Click Change password on next login to change the password when the user logs in to his system next time.

5 Click **OK**.

Working with Login and Logoff Scripts

You can bind a login or logoff script to the NSX Edge gateway.

Edit a Script

You can edit the type, description, and status of a login or logoff script that is bound to the NSX Edge gateway.

Procedure

1 In the **SSL VPN-Plus** tab, click **Login/Logoff Scripts** in the left panel.

2 Select a script and click the **Edit** ( ) icon.

3 Make the appropriate changes.

4 Click **OK**.

Delete a Script

You can delete a login or logoff script.

Procedure

1 In the **SSL VPN-Plus** tab, click **Login/Logoff Scripts** in the left panel.

2 Select a script and click the **Delete** ( ) icon.

Enable a Script

You must enable a script for it to work.

Procedure

1 In the **SSL VPN-Plus** tab, click **Login/Logoff Scripts** in the left panel.

2 Select a script and click the **Enable** ( ) icon.

Disable a Script

You can disable a login/logoff script.

Procedure

1 In the **SSL VPN-Plus** tab, click **Login/Logoff Scripts** in the left panel.

2 Select a script and click the **Disable** ( ) icon.

Change the Order of a Script

You can change the order of a script. For example, suppose you have a login script for opening gmail.com in Internet Explorer placed above a login script for opening yahoo.com. When the remote user logs in to SSL VPN, gmail.com is displayed before yahoo.com. If you now reverse the order of the login scripts, yahoo.com is displayed before gmail.com.

Procedure

1 In the **SSL VPN-Plus** tab, click **Login/Logoff Scripts** in the left panel.

2 Select the script that you want to change the order of and click the **Move Up** ( )or **Move Down** ( ) icon.

3 Click **OK**.

IPSec VPN Overview

NSX Edge supports site-to-site IPSec VPN between an NSX Edge instance and remote sites. Certificate authentication, preshared key mode, IP unicast traffic, and no dynamic routing protocol are supported between the NSX Edge instance and remote VPN routers.

NSX Edge supports Behind each remote VPN router, you can configure multiple subnets to connect to the internal network behind an NSX Edge through IPSec tunnels. These subnets and the internal network behind a NSX Edge must have address ranges that do not overlap.

You can deploy an NSX Edge agent behind a NAT device. In this deployment, the NAT device translates the VPN address of an NSX Edge instance to a publicly accessible address facing the Internet. Remote VPN routers use this public address to access the NSX Edge instance.

You can place remote VPN routers behind a NAT device as well. You must provide the VPN native address and the VPN Gateway ID to set up the tunnel. On both ends, static one-to-one NAT is required for the VPN address.

You can have a maximum of 64 tunnels across a maximum of 10 sites. The following IPSec VPN algorithms are supported:

- 3DES192-CBC
- AES128-CBC

- AES128-CBC
- AES128-CBC
- AES128-CBC
- DH-2
- DH-5

For IPSec VPN configuration examples, see Chapter 15, "NSX Edge VPN Configuration Examples," on page 199.

Configuring IPSec VPN Service

You can set up an NSX Edge tunnel between a local subnet and a peer subnet.

1 Enable IPSec VPN Service on page 86
You must enable the IPSec VPN service for traffic to flow from the local subnet to the peer subnet.

2 Specify Global IPSec VPN Configuration on page 86
This enables IPSec VPN on the NSX Edge instance.

3 Enable Logging for IPSec VPN on page 87
You can enable logging of all IPSec VPN traffic.

4 Configure IPSec VPN Parameters on page 87
You must configure at least one external IP address on the NSX Edge to provide IPSec VPN service.

Enable IPSec VPN Service

You must enable the IPSec VPN service for traffic to flow from the local subnet to the peer subnet.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **VPN** tab.

5 Click **IPSec VPN**.

6 Click **Enable**.

Specify Global IPSec VPN Configuration

This enables IPSec VPN on the NSX Edge instance.

Prerequisites

If you want to enable certificate authentication, server certificates, CA certificates, or CRLs must have been imported.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **VPN** tab.

5 Click **IPSec VPN**.

6 Click **Change** next to Global configuration status.

7 Type a global pre-shared key for those sites whose peer endpoint is set to any and select **Display shared key** to display the key.

8 Select Enable certificate authentication and select the appropriate certificate.

9 Click **OK**.

Enable Logging for IPSec VPN

You can enable logging of all IPSec VPN traffic.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **VPN** tab.

5 Click **IPSec VPN**.

6 Click next to **Logging Policy** and click **Enable logging** to log the traffic flow between the local subnet and peer subnet and select the logging level.

7 Select the log level and click **Publish Changes** .

Configure IPSec VPN Parameters

You must configure at least one external IP address on the NSX Edge to provide IPSec VPN service.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click the **VPN** tab.

5 Click **IPSec VPN**.

6 Click the **Add** ( ) icon.

7 Type a name for the IPSec VPN.

8 Type the IP address of the NSX Edge instance in **Local Id**. This will be the peer Id on the remote site.

9 Type the IP address of the local endpoint.

If you are adding an IP to IP tunnel using a pre-shared key, the local Id and local endpoint IP can be the same.

10 Type the subnets to share between the sites in CIDR format. Use a comma separator to type multiple subnets.

11 Type the Peer Id to uniquely identify the peer site. For peers using certificate authentication, this ID must be the common name in the peer's certificate. For PSK peers, this ID can be any string. VMware recommends that you use the public IP address of the VPN or a FQDN for the VPN service as the peer ID.

12 Type the IP address of the peer site in Peer Endpoint. If you leave this blank, NSX Edge waits for the peer device to request a connection.

13 Type the internal IP address of the peer subnet in CIDR format. Use a comma separator to type multiple subnets.

14 Select the Encryption Algorithm.

15 In Authentication Method, select one of the following:

Option	Description
PSK (Pre Shared Key)	Indicates that the secret key shared between NSX Edge and the peer site is to be used for authentication. The secret key can be a string with a maximum length of 128 bytes.
Certificate	Indicates that the certificate defined at the global level is to be used for authentication.

16 Type the shared key in if anonymous sites are to connect to the VPN service.

17 Click **Display Shared Key** to display the key on the peer site.

18 In Diffie-Hellman (DH) Group, select the cryptography scheme that will allow the peer site and the NSX Edge to establish a shared secret over an insecure communications channel.

19 In Extension, type one of the following:

- securelocaltrafficbyip=*IPAddress* to re-direct Edge's local traffic over the IPSec VPN tunnel. This is the default value.
- passthroughSubnets=*PeerSubnetIPAddress* to support overlapping subnets .

20 Click **OK**.

NSX Edge creates a tunnel from the local subnet to the peer subnet.

What to do next

Enable the IPSec VPN service.

Edit IPSec VPN Service

You can edit an IPSec VPN service.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click **VPN** tab.

5 Click **IPSec VPN**.

6 Select the IPSec service that you want to edit.

7 Click the **Edit** ( ) icon.

8 Make the appropriate edits.

9 Click **OK**.

Disable IPSec Service

You can disable an IPSec service.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click **VPN** tab.

5 Click **IPSec VPN**.

6 Select the IPSec service that you want to disable.

7 Click the **Disable** () icon.

Delete IPSec Service

You can delete an IPSec service.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click **VPN** tab.

5 Click **IPSec VPN**.

6 Select the IPSec service that you want to delete.

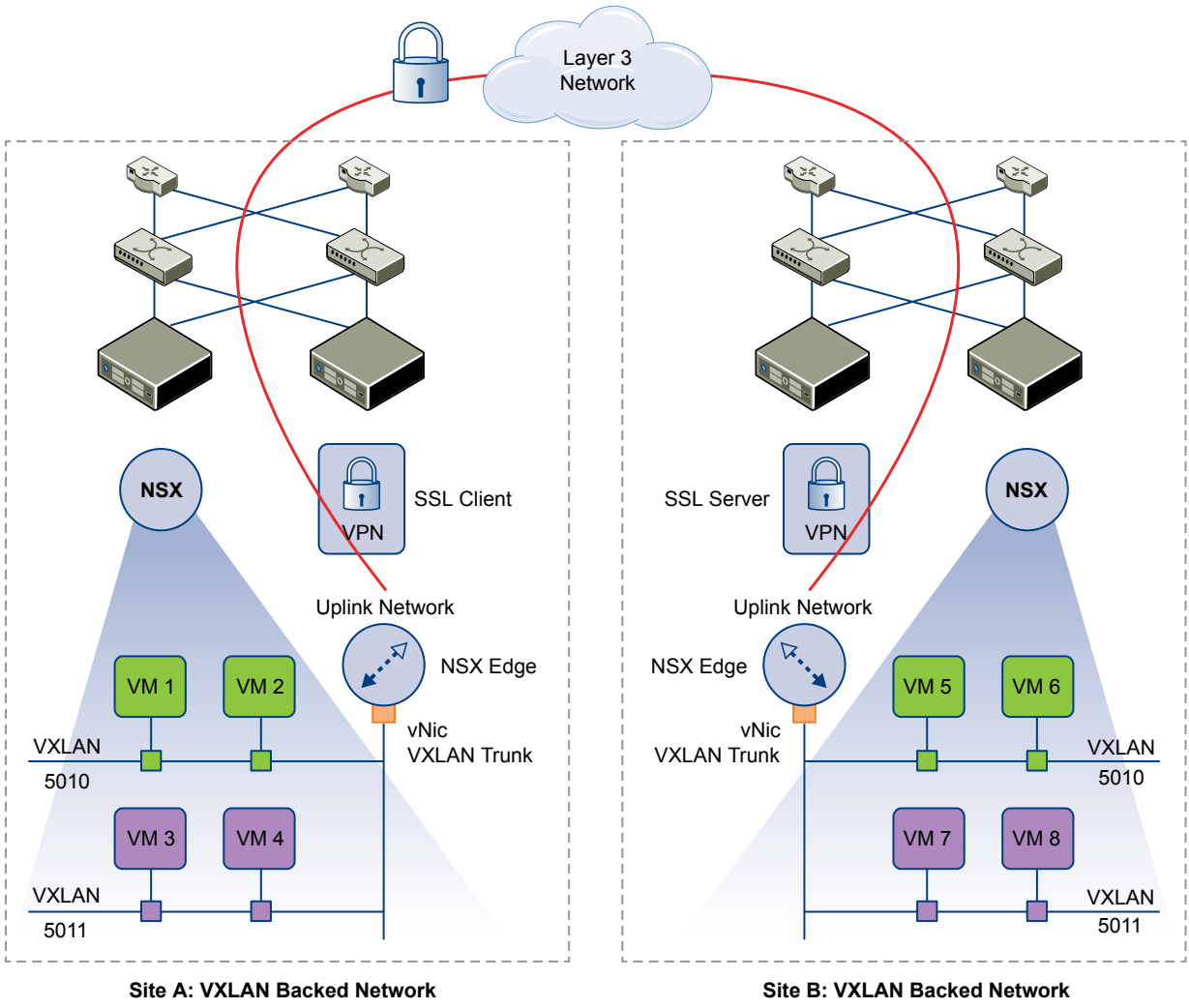
7 Click the **Delete** () icon.

L2 VPN Overview

With L2 VPN, you can stretch multiple logical networks (both VLAN and VXLAN) across geographical sites. In addition, you can configure multiple sites on an L2 VPN server. Virtual machines remain on the same subnet when they are moved between sites and their IP addresses do not change. Egress optimization enables Edge to route any packets sent towards the Egress Optimization IP address locally, and bridge everything else.

L2 VPN thus allows enterprises to seamlessly migrate workloads backed by VXLAN or VLAN between physically separated locations. For cloud providers, L2 VPN provides a mechanism to on-board tenants without modifying existing IP addresses for workloads and applications.

Figure 6-1. Extending VXLAN across Multiple Sites using L2 VPN

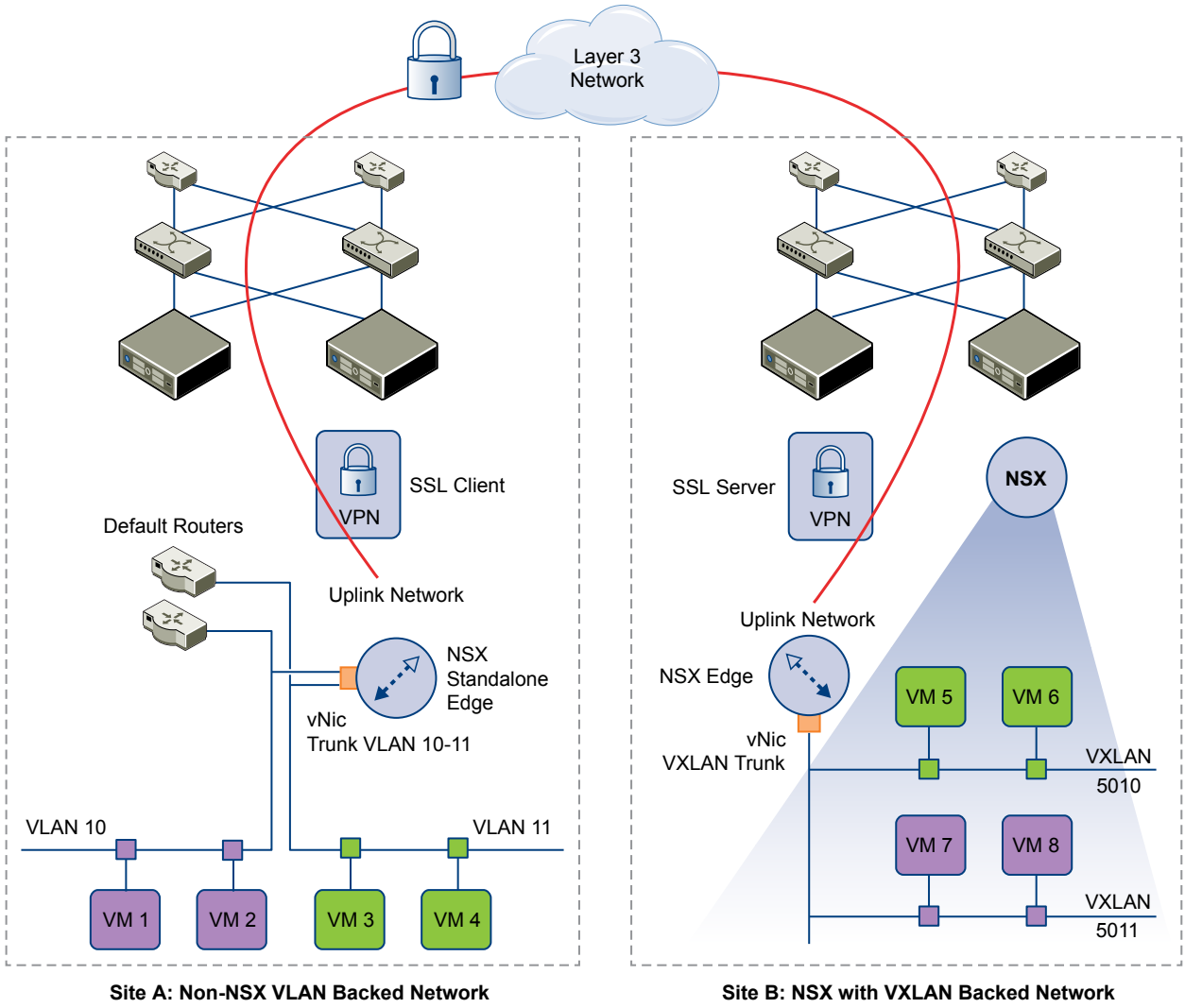


The L2 VPN client and server learn the MAC addresses on both local and remote sites based on the traffic flowing through them. Egress optimization maintains local routing since the default gateway for all virtual machines are always resolved to the local gateway using firewall rules. Virtual machines that have been moved to Site B can also access L2 segments that are not stretched on Site A.

If one of the sites is not backed by NSX, a standalone NSX Edge can be deployed on that site.

In the following graphic, L2 VPN stretches network VLAN 10 to VXLAN 5010 and VLAN 11 to VXLAN 5011. So VM 1 bridged with VLAN 10 can access VMs 2, 5, and 6.

Figure 6-2. Extending Non-NSX Site with VLAN Based Network to NSX-Site with VXLAN Based Network



Configuring L2 VPN

To stretch your network using L2 VPN, you configure an L2 VPN server (destination Edge) and an L2 VPN client (source Edge). You must then enable the L2 VPN service on both the server and the client.

Prerequisites

A sub interface must have been added on a trunk interface of the NSX Edge. See "Add a Sub Interface," on page 172.

Procedure

1 Configure L2 VPN Server on page 92

The L2 VPN server is the destination NSX Edge to which the client is to be connected.

2 Add Peer Sites on page 92

You can connect multiple sites to the L2 VPN server.

3 Enable L2 VPN Service on Server on page 93

You must enable the L2 VPN service on the L2 VPN server (destination NSX Edge).

4 Configure L2 VPN Client on page 93

The L2 VPN client is the source NSX Edge that initiates communication with the destination Edge (L2 VPN server).

5 Enable L2 VPN Service on Client on page 94

You must enable the L2 VPN service on the L2 VPN client (source NSX Edge).

Configure L2 VPN Server

The L2 VPN server is the destination NSX Edge to which the client is to be connected.

Procedure

1 In the **L2 VPN** tab, select **Server** and click **Change**.

2 In **Listener IP**, type the primary or secondary IP address of an external interface of the NSX Edge.

3 The default port for the L2 VPN service is 443. Edit this if required.

4 Select the encryption algorithm for communication between the server and the client.

The following algorithms are supported:

- RC4-MD5
- AES128-SHA
- AES256-SHA
- DES-CBC3-SHA
- AES128-GCM-SHA256
- NULL-MD5

5 Select the certificate to be bound to SSL VPN server.

6 Click **OK**.

Add Peer Sites

You can connect multiple sites to the L2 VPN server.

Procedure

1 In the L2 VPN tab, ensure that the **L2 VPN Mode** is **Server**.

2 In **Site Configuration Details**, click the **Add** icon.

3 Type a unique name for the peer site.

4 Type the user name and password with which the peer site is to be authenticated. User credentials on the peer site should be the same as those on the client side.

5 In **Stretched Interfaces**, click **Select Sub Interfaces** to select the sub interfaces to be stretched with the client.

a In Select Object, select the trunk interface for the Edge.

Sub interfaces configured on the trunk vNIC are displayed.

b Double-click the sub interfaces to be stretched.

c Click **OK**.

6 If the default gateway for virtual machines is same across the two sites, type the gateway IP addresses for which the traffic should be locally routed or for which traffic is to be blocked over the tunnel in **Egress Optimization Gateway Address**.

7 Click **OK** and then click **Publish Changes**.

Enable L2 VPN Service on Server

You must enable the L2 VPN service on the L2 VPN server (destination NSX Edge).

Procedure

1 For the destination NSX Edge, navigate to **Manage > VPN > L2 VPN**.

2 In **L2VPN Service Configuration**, click **Enable**.

What to do next

Create NAT or firewall rule on the internet facing firewall side to enable the client and server to connect to each other.

Configure L2 VPN Client

The L2 VPN client is the source NSX Edge that initiates communication with the destination Edge (L2 VPN server).

You can also configure a standalone Edge as the L2 VPN client. See "Configure Standalone Edge as L2 VPN Client," on page 94.

Procedure

1 In the L2 VPN tab, set the **L2 VPN Mode** to **Client** and click **Change**.

2 Type the address of the L2 VPN server to which this client is to be connected. The address can be the host name or IP address.

3 If required, edit the default port to which the L2 VPN client should connect to.

4 Select the encryption algorithm for communicating with the server.

5 In **Stretched Interfaces**, click **Select Sub Interfaces** to select the sub interfaces to be stretched to the server.

   a In **Select Object**, select the trunk interface for the Edge.

      Sub interfaces configured on the trunk vNIC are displayed.

   b Double-click the sub interfaces to be stretched.

   c Click **OK**.

6 Type a description.

7 In **Egress Optimization Gateway Address**, type the gateway IP address of the sub interfaces or the IP addresses to which traffic should not flow over the tunnel.

8 In **User Details**, type the user credentials to get authenticated at the server..

9 Click the **Advanced** tab.

   If the client NSX Edge does not have direct access to the internet and needs to reach the source (server) NSX Edge via a proxy server, specify **Proxy Settings**.

10 To enable only secure proxy connections, select **Enable Secure Proxy**.

11 Type the proxy server address, port, user name, and password.

12 To enable server certificate validation, select **Validate Server Certificate** and select the appropriate CA certificate.

13 Click **OK** and then click **Publish Changes**.

What to do next

Ensure that the internet facing firewall allows traffic to flow from L2 VPN Edge to the internet. The destination port is 443.

Enable L2 VPN Service on Client

You must enable the L2 VPN service on the L2 VPN client (source NSX Edge).

Procedure

1 For the source NSX Edge, navigate to **Manage > VPN > L2 VPN**.

2 In **L2VPN Service Configuration**, click **Enable**.

What to do next

- Create NAT or firewall rule on the internet facing firewall side to enable the client and server to connect to each other.
- If a trunk vNic backed by standard portgroup is being stretched, enable L2 VPN traffic manually by the following steps:

  a Set **Promiscuous mode** to **Accept**.

  b Set **Forged Transmits** to **Accept**.

  For more information, see *ESXi and vCenter Server 5.5 Documentation*.

Configure Standalone Edge as L2 VPN Client

If one of the sites that you want to stretch is not backed by NSX, you can deploy a standalone Edge as the L2 VPN client on that site.

Procedure

1 Copy the `NSX-l2vpn-client.ovf` file to your computer.

2 Using vSphere Web Client, log in to the vCenter Server that manages the non-NSX environment.

3 Select **Datacenters > Hosts and Clusters > Hosts**.

4 Right-click the host where you want to install the standalone Edge and select **Deploy OVF Template**.

5 Enter the URL to download and install the OVF file from the internet or click **Browse** to locate the folder on your computer that contains the standalone Edge OVF file and click **Next**.

6 On the OVF Template Details page, verify the template details and click **Next**.

7 On the Name and Location page, type a name for the standalone Edge and select the location where you want to deploy. Then click **Next**.

8 On the Network Mapping page, select the network in your environment that you want to map to the OVF network. Then click **Next**.

9 On the Properties page, specify the following values.

  a Type and retype the admin CLI password.

  b Type and retype the root CLI password.

  c Type the uplink IP address, prefix length, default gateway, and DNS IP address.

  d Select the cipher to be used for authentication.

  e To enable Egress Optimization, type the gateway IP addresses for which traffic should be locally routed or for which traffic is to be blocked over the tunnel.

f Type the L2 VPN server address.

g Type the user name and password with which the peer site is to be authenticated.

h In VLAN ID, type VLAN ID(s) of the network(s) you want to stretch. a tunnel ID. You can list the VLAN IDs as a comma separated list or range. For example, 2,3,10-20.

If you want to change the VLAN ID of the network before stretching it to the standalone Edge site, you can type the VLAN ID of the network and then type the tunnel ID in brackets. For example, 2(100),3(200). The Tunnel ID is used to map the networks that are being stretched. However, you cannot specify the tunnel ID with a range. So this would not be allowed: 10(100)-14(104). You would need to rewrite this as 10(100),11(101),12(102),13(103),14(104).

i If the standalone NSX Edge does not have direct access to the internet and needs to reach the source (server) NSX Edge via a proxy server, type the proxy address, port, user name, and password.

j Click **Next**.

10 On the Ready to complete page, review the standalone Edge settings and click **Finish**.

Power on the standalone Edge virtual machine.

View L2 VPN Statistics

You can view L2 VPN statistics such as tunnel status, bytes sent and received etc. for the source and destination NSX Edge.

Procedure

1 In the L2 VPN tab. ensure that the **L2 VPN Mode** is **Client**.

2 Click **Fetch Status** and expand **Tunnel Status**.

If the L2 VPN server has multiple peer sites, statistics are displayed for all the peer sites.

What to do next

To see the networks configured on a trunk interface, navigate to **Manage > Settings > Interfaces** for the Edge and click **Trunk** in the Type column.

Logical Load Balancer 7

The NSX Edge load balancer enables network traffic to follow multiple paths to a specific destination. It distributes incoming service requests evenly among multiple servers in such a way that the load distribution is transparent to users. Load balancing thus helps in achieving optimal resource utilization, maximizing throughput, minimizing response time, and avoiding overload. NSX Edge provides load balancing up to Layer 7.

You map an external, or public, IP address to a set of internal servers for load balancing. The load balancer accepts TCP, HTTP, or HTTPS requests on the external IP address and decides which internal server to use. Port 8090 is the default listening port for TCP, port 80 is the default port for HTTP, and port 443 is the default port for HTTPs.

You must have a working NSX Edge instance before you can load balancing. For information on setting up NSX Edge, see "NSX Edge Operations," on page 166.

For information on configuring an NSX Edge certificate, see "Working with Certificates," on page 166.

This chapter includes the following topics:

- "Set Up Load Balancing," on page 97
- "Working with Application Profiles," on page 105
- "Working with Service Monitors," on page 105
- "Working with Server Pools," on page 106
- "Working with Virtual Servers," on page 106
- "Working with Application Rules," on page 107

Set Up Load Balancing

The NSX Edge load balancer distributes network traffic across multiple servers to achieve optimal resource utilization.

You begin by setting global options for the load balancer. You then create an application profile to define the behavior of a particular type of network traffic. Next, you create a service monitor to define health check parameters for the load balancer.

You now create a server pool consisting of backend server members and associate a service monitor with the pool to manage and share the backend servers flexibly and efficiently.

When the virtual server receives a request, it chooses the appropriate pool to distribute the traffic comprising one or more members based on the associated algorithm.

Each pool is monitored by the associated service monitor. When the load balancer detects a problem with a pool member, it is marked as down.

Configure Load Balancer Service

You can specify global load balancer configuration parameters.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click the **Load Balancer** tab.

5 Click **Edit**.

6 Select the check boxes next to the options you want to enable.

Option	Description
Enable Loadbalancer	Allows the NSX Edge load balancer to distribute traffic to internal servers for load balancing.
Enable Service Insertion	Allows the load balancer to work with third party vendor services. If you have a third party vendor load balancer service deployed in your environment, see "Using a Partner Load Balancer," on page 141.
Acceleration Enabled	When enabled, the NSX Edge load balancer uses the faster L4 LB engine rather than L7 LB engine.
Logging	NSX Edge load balancer collects traffic logs. You can also choose the log level.

7 Click **OK**.

Create a Service Monitor

You create a service monitor to define health check parameters for a particular type of network traffic. When you associate a service monitor with a pool, the pool members are monitored according to the service monitor parameters

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click the **Load Balancer** tab.

5 In the left navigation panel, click **Service Monitoring**.

6 Click the **Add** icon.

7 Type a name for the service monitor.

8 Type the interval at which a server is to be pinged.

9 Type the maximum time in seconds within which a response from the server must be received.

10 Type the number of times the server must be pinged before it is declared down.

11 Select the way in which you want to send the health check request to the server.

12 For HTTP and HTTPS traffic, perform the steps below.

a In **Expect**, type the string that the monitor expects to match in the status line of HTTP response (for example, HTTP/1.1).

b Select the method to be used to detect server status.

c Type the URL to be used in the sample request.

d If you selected the POST method, type the data to be sent.

e In **Receive**, type the string to be matched in the response content.

If **Expect** is not matched, the monitor does not try to match the **Receive** content.

f (Optional) In Extension, type advanced monitor parameters as key=value pairs.

For example, warning=10 indicates that if a server does not respond within 10 seconds, its status is set as warning.

13 Click **OK**.

What to do next

Associate a service monitor with a pool.

Add a Server Pool

You can add a server pool to manage and share backend servers flexibly and efficiently. A pool manages load balancer distribution methods and has a service monitor attached to it for health check parameters.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click the **Load Balancer** tab.

5 In the left navigation panel, click **Pools**.

6 Type a name and description for the load balancer pool.

7 Select a balancing method for each enabled service.

Option	Description
IP_HASH	Selects a server based on a hash of the source and destination IP address of each packet.
LEAST_CONN	Distributes client requests to multiple servers based on the number of connections already on the server. New connections are sent to the server with the fewest connections.
ROUND_ROBIN	Each server is used in turn according to the weight assigned to it. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed.
URI	The left part of the URI (before the question mark) is hashed and divided by the total weight of the running servers. The result designates which server will receive the request. This ensures that a URI is always directed to the same server as long as no server goes up or down.

8 Add members to the pool.

a Click the **Add** icon.

b Type the name and IP address of the server member.

c Type the port where the member is to receive traffic on and the monitor port where the member is to receive health monitor pings.

d In **Weight**, type the proportion of traffic this member is to handle.

e Type the maximum number of connections the member can handle.

f Type the minimum number of connections a member should handle before traffic is redirected to the next member.

g Click **OK**.

9 **Transparent** indicates whether client IP addresses are visible to the backend servers. If **Transparent** is not selected (default value), backend servers see the traffic source IP as a Load balancer internal IP. If **Transparent** is selected, source IP is the real client IP and NSX Edge must be set as the default gateway to ensure that return packets go through the NSX Edge device.

10 Click **OK**.

Create an Application Profile

You create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click the **Load Balancer** tab.

5 In the left navigation panel, click **Application Profiles**.

6 Click the **Add** icon.

7 Type a name for the profile and select the traffic type for which you are creating the profile.

8 Type the URL to which you want to re-direct HTTP traffic. For example, you can direct traffic from `http://myweb.com` to `https://myweb.com`.

9 Specify persistence for the profile. Persistence tracks and stores session data, such as the specific pool member that serviced a client request. This ensures that client requests are directed to the same pool member throughout the life of a session or during subsequent sessions.

Cookie persistence inserts a cookie to uniquely identify the session the first time a client accessed the site and then refers to that cookie in subsequent requests to persist the connection to the appropriate server. Type the cookie name and select the mode by which the cookie should be inserted.

SOURCEIP persistence tracks sessions based on the source IP address. When a client requests a connection to a virtual server that supports source address affinity persistence, the load balancer checks to see if that client previously connected, and if so, returns the client to the same pool member.

Microsoft Remote Desktop Protocol (**MSRDP**) persistence maintains persistent sessions between Windows clients and servers that are running the Microsoft Remote Desktop Protocol (RDP) service. The recommended scenario for enabling MSRDP persistence is to create a load balancing pool that consists of members running Windows Server 2003 or Windows Server 2008, where all members belong to a Windows cluster and participate in a Windows session directory.

Traffic Type	Persistence Method Supported
TCP	SOURCEIP, MSRDP
HTTP	Cookie, SOURCEIP
HTTPS	Cookie, ssl_session_id (SSL Passthrough enabled) , SOURCEIP
UDP	SOURCEIP

10 If you are creating a profile for HTTPS traffic, complete the steps below. The following HTTPS traffic pattern are allowed.

Client -> HTTPS -> LB (terminate SSL) -> HTTP -> servers

Client -> HTTPS -> LB (terminate SSL) -> HTTPS -> servers

Client -> HTTPS-> LB (SSL passthrough) -> HTTPS -> servers

Client -> HTTP-> LB -> HTTP -> servers

a Select **Insert X-Forwarded-For HTTP** header for identifying the originating IP address of a client connecting to a web server through the load balancer.

b Select the certificate/CAs/CRLs used to decrypt HTTPS traffic in **Virtual Server Certificates**.

c Define the certificate/CAs/CRLs used to authenticate the load balancer from the server side in **Pool Certificates**.

11 In **Cipher**, select the cipher algorithms (or cipher suite) negotiated during the SSL/TLS handshake.

12 Specify whether client authentication is to be ignored or required. If set to required, the client must provide a certificate after the request or the handshake is aborted.

13 Click **OK**.

Add an Application Rule

You can write an application rule to directly manipulate and manage IP application traffic. For application rule examples, see .

"Application Rule Examples," on page 102.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click the **Load Balancer** tab.

5 In the left navigation panel, click **Application Rules** and click the **Add** icon.

6 Type the name and script for the rule.

For information on the application rule syntax, see http://cbonte.github.io/haproxy-dconv/configuration-1.5.html.

7 Click **OK**.

Application Rule Examples

HTTP/HTTPS redirection based on condition

An application profile allows you to specify HTTP/HTTPS redirection, which always redirects traffic regardless of the request URLs. You also have the flexibility to specify the conditions in which HTTP/HTTPS traffic should be redirected.

```
move the login URL only to HTTPS.
acl clear dst_port 80
acl secure dst_port 8080
acl login_page url_beg /login
acl logout url_beg /logout
acl uid_given url_reg /login?userid=[^&]+
acl cookie_set hdr_sub(cookie) SEEN=1
redirect prefix https://mysite.com set-cookie SEEN=1 if !cookie_set
redirect prefix https://mysite.com if login_page !secure
redirect prefix http://mysite.com drop-query if login_page !uid_given
redirect location http://mysite.com/ if !login_page secure
 redirect location/ clear-cookie USERID= if logout
```

Routing by domain name

You can create an application rule to direct requests to a specific load balancer pool according to domain name. The following rule direct requests to foo.com to pool_1, and requests to bar.com to pool_2.

```
acl is_foo hdr_dom(host) -i foo
  acl is_bar hdr_dom(host) -i bar
  use_backend pool_1 if is_foo
  use backend pool_2  if is_bar
```

Microsoft RDP load balancing and protection

In the following sample scenario, the load balancer balances a new user to the less loaded server and also resumes a broken session. The NSX Edge internal interface IP for this scenario is 10.0.0.18, internal interface IP is 192.168.1.1, and the virtual servers are 192.168.1.100, 192.168.1.101, and 192.168.1.102.

1 Create a application profile for TCP traffic with MSRDP persistence.

2 Create a TCP health monitor (tcp_monitor).

3 Create a pool (named rdp-pool) with 192.168.1.100:3389, 192.168.1.101:3389 and 192.168.1.102:3389 as members.. Associate tcp_monitor to this pool.

4 Create the following application rule.

```
tcp-request content track-sc1 rdp_cookie(mstshash) table rdp-pool
tcp-request content track-sc2 src table ipv4_ip_table

#   each single IP can have up to 2 connections on the VDI infrastructure
tcp-request content reject if { sc2_conn_cur ge 2 }

#   each single IP can try up to 5 connections in a single minute
tcp-request content reject if { sc2_conn_rate ge 10 }

# Each user is supposed to get a single active connection at a time, block the second one
tcp-request content reject if { sc1_conn_cur ge 2 }
```

```
    # if a user tried to get connected at least 10 times over the last minute,
    # it could be a brute force
    tcp-request content reject if { sc1_conn_rate ge 10 }
```

5 Create a virtual server (named rdp-vs). Associate the application profile to this virtual server and add the application rule created in step 4.

Advanced Logging

By default, NSX load balancer supports basical logging. You can create an application rule as follows to view more detailed logging messages for troubleshooting.

```
 # log the name of the virtual server
 capture request  header Host len 32

 # log the amount of data uploaded during a POST
 capture request  header Content-Length len 10
# log the beginning of the referrer
capture request  header Referer len 20

# server name (useful for outgoing proxies only)
capture response header Server len 20

# logging the content-length is useful with "option logasap"
capture response header Content-Length len 10

# log the expected cache behaviour on the response
capture response header Cache-Control len 8

# the Via header will report the next proxy's name
 capture response header Via len 20

# log the URL location during a redirection
capture response header Location len 20
```

After you associate the application rule to the virtual server, logs include detailed messages such as the following example.

```
2013-04-25T09:18:17+00:00 edge-187 loadbalancer[18498]: [org1]: 10.117.7.117 - -
[25/Apr/2013:09:18:16 +0000] "GET /favicon.ico HTTP/1.1" 404 1440 "" "" 51656 856 "vip-http-
complete"
"pool-http-complete" "m2" 145 0 1 26 172 --NI 1 1 0 0 0 0 0 "" "" "10.117.35.187" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.31
(KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "Apache/2.2.15 (Linux" ""

2013-04-25T09:18:17+00:00 edge-187 loadbalancer[18498]: [org1]: 10.117.7.117 - -
[25/Apr/2013:09:18:16 +0000] "GET /favicon.ico HTTP/1.1" 404 1440 "" "" 51657 856 "vip-http-
complete"
"pool-http-complete" "m2" 412 0 0 2 414 --NI 0 0 0 0 0 0 0 "" "" "10.117.35.187" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.31
(KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "Apache/2.2.15 (Linux" ""
```

To troubleshoot the HTTPS traffic, you may need to add more rules. Most web application use 301/302 responses with a location header to redirect the client to a page (most of the time after a login or a POST call) and also require an application cookie. So your application server may have difficulty in getting to know client connection information and may not be able to provide the correct responses: it may even stop the application from working.

To allow the web application to support SSL offloading, add the following rule.

```
# See clearly in the log if the application is setting up response for HTTP or HTTPS
capture response header Location   len 32
capture response header Set-Cookie len 32

# Provde client side connection info to application server over HTTP header
http-request set-header X-Forwarded-Proto https if  { ssl_fc }
http-request set-header X-Forwarded-Proto http  if !{ ssl_
```

The load balancer inserts the following header when the connection is made over SSL.

```
X-Forwarded-Proto: https
```

The load balancer inserts the following header when the connection is made over HTTP.

```
X-Forwarded-Proto: http
```

Add Virtual Servers

Add an NSX Edge internal or uplink interface as a virtual server.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click the **Load Balancer** tab.

5 In the left navigation panel, click **Virtual Servers**.

6 Click the **Add** ( ) icon.

7 Type a name for the virtual server.

8 (Optional) Type a description for the virtual server.

9 Type the IP address that the load balancer is listening on. Type the protocol that the virtual server will handle.

10 Type the protocol that the virtual server will handle.

11 Type the port number that the load balancer will listen on.

12 Select the application profile to be associated with the virtual server. You can associate only an application profile with the same protocol as the virtual server that you are adding.

The services supported by the selected pool appear.

13 Select the application rule to be associated with the virtual server.

14 In **Connection Limit**, type the maximum concurrent connections that the virtual server can process.

15 In **Connection Rate Limit**, type the maximum incoming new connection requests per second.

16 Click **OK**.

Working with Application Profiles

Delete an Application Profile

You can delete an application profile.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click the **Load Balancer** tab.

5 In the left navigation panel, click **Application Profiles**.

6 Select a profile and click the **Delete** icon.

Edit an Application Profile

You can edit an application profile.

Working with Service Monitors

Edit a Service Monitor

You can edit a service monitor.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click the **Load Balancer** tab.

5 In the left navigation panel, click **Service Monitoring**.

6 Select a service monitor and click the **Edit** icon.

7 Make the appropriate changes and click **OK**.

Delete a Service Monitor

You can delete a service monitor.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click the **Load Balancer** tab.

5 In the left navigation panel, click **Service Monitoring**.

6 Select a service monitor and click the **Delete** icon.

Working with Server Pools

Edit a Server Pool

You can edit a server pool.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click the **Load Balancer** tab.

5 Ensure that you are in the Pool tab.

6 Select the pool to edit.

7 Click the **Edit** ( ) icon.

8 Make the appropriate changes and click **Finish**.

Delete a Server Pool

You can delete a server pool.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click the **Load Balancer** tab.

5 Ensure that you are in the Pool tab.

6 Select the pool to delete

7 Click the **Delete** ( ) icon.

Working with Virtual Servers

Edit a Virtual Server

You can edit a virtual server.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click the **Load Balancer** tab.

5 Click **Virtual Servers** tab.

6 Select the virtual server to edit.

7 Click the **Edit** () icon.

8 Make the appropriate changes and click **Finish**.

Delete a Virtual Server

You can delete a virtual server.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click the **Load Balancer** tab.

5 Click **Virtual Servers** tab.

6 Select the virtual server to delete.

7 Click the **Delete** () icon.

Working with Application Rules

Edit an Application Rule

You can edit an application rule.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click the **Load Balancer** tab.

5 In the left navigation panel, click **Application Rules**.

6 Select a rule and click the **Edit** icon.

7 Make the appropriate changes and click **OK**.

Delete an Application Rule

You can delete an application rule.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click **Manage** and then click the **Load Balancer** tab.

5 In the left navigation panel, click **Application Profiles**.

6 Select a profile and click the **Delete** icon.

8 Other Edge Services

An NSX services gateway offers IP address pooling and one-to-one static IP address allocation and external DNS server configuration.

You must have a working NSX Edge instance before you can use any of the above services. For information on setting up NSX Edge, see "NSX Edge Operations," on page 166.

This chapter includes the following topics:

- "Managing DHCP Service," on page 109
- "Configuring DHCP Relay," on page 112
- "Configure DNS Servers," on page 113

Managing DHCP Service

NSX Edge supports IP address pooling and one-to-one static IP address allocation. Static IP address binding is based on the vCenter managed object ID and interface ID of the requesting client.

NSX Edge DHCP service adheres to the following guidelines:

- Listens on the NSX Edge internal interface for DHCP discovery.
- Uses the IP address of the internal interface on NSX Edge as the default gateway address for all clients, and the broadcast and subnet mask values of the internal interface for the container network.

You must restart the DHCP service on client virtual machines in the following situations:

- You changed or deleted a DHCP pool, default gateway, or DNS server.
- You changed the internal IP address of the NSX Edge instance.

Add a DHCP IP Pool

DHCP service requires a pool of IP addresses. An IP pool is a sequential range of IP addresses within the network. Virtual machines protected by NSX Edge that do not have an address binding are allocated an IP address from this pool. An IP pool's range cannot intersect one another, thus one IP address can belong to only one IP pool.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **DHCP** tab.

5 Click the **Add** ( ) icon.

6 Configure the pool.

Option	Action
Auto Configure DNS	Select to use the DNS service configuration for the DHCP binding.
Lease never expires	Select to bind the address to the MAC address of the virtual machine forever. If you select this, **Lease Time** is disabled.
Start IP	Type the starting IP address for the pool.
End IP	Type the ending IP address for the pool.
Domain Name	Type the domain name of the DNS server. This is optional.
Primary Name Server	If you did not select **Auto Configure DNS**, type the **Primary Nameserver** for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution. This is optional.
Secondary Name Server	If you did not select **Auto Configure DNS**, type the **Secondary Nameserver** for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution. This is optional.
Default Gateway	Type the default gateway address. If you do not specify the default gateway IP address, the internal interface of the NSX Edge instance is taken as the default gateway. This is optional.
Lease Time	Select whether to lease the address to the client for the default time (1 day), or type a value in seconds. You cannot specify the lease time if you selected **Lease never expires**. This is optional.

7 Click **OK**.

Enable the DHCP Service

Enable the DHCP service to allow NSX Edge to automatically assign an IP address to a virtual machine from a defined IP pool.

Prerequisites

A DHCP IP pool must have been added.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **DHCP** tab.

5 Click **Enable**.

6 Select **Enable logging** if required and select the log level.

7 Click **Publish Changes**.

What to do next

Create an IP pool and bindings.

Edit DHCP IP Pool

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **DHCP** tab.

5 Select a DHCP pool and click the **Edit** icon.

6 Make the appropriate changes and click **OK**.

Add a DHCP Static Binding

If you have services running on a virtual machine and do not want the IP address to be changed, you can bind an IP address to the MAC address of a virtual machine. The IP address you bind must not overlap an IP pool.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **DHCP** tab.

5 Select **Bindings** from the left panel.

6 Click the **Add** ( ) icon.

7 Configure the binding.

Option	Action
Auto Configure DNS	Select to use the DNS service configuration for the DHCP binding.
Lease never expires	Select to bind the address to the MAC address of the virtual machine forever.
Interface	Select the NSX Edge interface to bind.
VM Name	Select the virtual machine to bind.
VM vNIC Index	Select the virtual machine NIC to bind to the IP address.
Host Name	Type the host name of the DHCP client virtual machine.
IP Address	Type the address to which to bind the MAC address of the selected virtual machine.
Domain Name	Type the domain name of the DNS server.
Primary Name Server	If you did not select **Auto Configure DNS**, type the **Primary Nameserver** for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution.
Secondary Name Server	If you did not select **Auto Configure DNS**, type the **Secondary Nameserver** for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution.
Default Gateway	Type the default gateway address. If you do not specify the default gateway IP address, the internal interface of the NSX Edge instance is taken as the default gateway.
Lease Time	If you did not select **Lease never expires**, select whether to lease the address to the client for the default time (1 day), or type a value in seconds.

8 Click **Add**.

9 Click **Publish Changes**.

Edit DHCP Binding

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **DHCP** tab.

5 Select **Bindings** from the left panel and click the binding to edit.

6 Click the Edit icon.

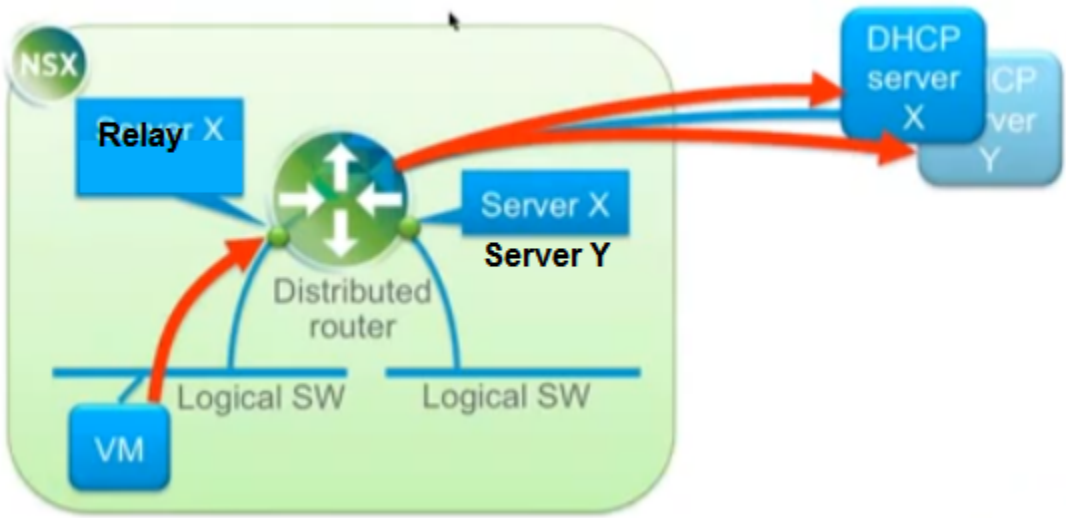
7 Make the appropriate changes and click **OK**.

Configuring DHCP Relay

Dynamic Host Configuration Protocol (DHCP) relay enables you to leverage your existing DHCP infrastructure from within NSX without any interruption to the IP address management in your environment. DHCP messages are relayed from virtual machine(s) to the designated DHCP server(s) in the physical world. This enables IP addresses within NSX to continue to be in synch with IP addresses in other environments.

DHCP configuration is applied on the logical router port and can list several DHCP servers. Requests are sent to all listed servers. While relaying the DHCP request from the client, the relay adds a Gateway IP Address to the request. The external DHCP server uses this gateway address to match a pool and allocate an IP address for the request. The gateway address must belong to a subnet of the NSX port on which the relay is running.

You can specify a different DHCP server for each logical switch and can configure multiple DHCP servers on each logical router to provide support for multiple IP domains.



NOTE

- DHCP relay does not support overlapping IP address space (option 82).
- DHCP Relay and DHCP service cannot run on a port/vNic at the same time. If a relay agent is configured on a port, a DHCP pool cannot be configured on the subnet(s) of this port.

Add DHCP Relay Server

Add the external relay server(s) to which you want the DHCP messages to be relayed to. The relay server can be an IP set, IP address block, domain, or a combination of all of these. Messages are relayed to each listed DHCP server.

Procedure

1 In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.

2 Double-click the appropriate Edge and ensure that that you are in the **Manage > DHCP** tab.

3 Click **Edit** next to **DHCP Relay Global Configuration**.

4 To add an IP set as the a server:

a Click the **Add** icon and select the IP set.

b Move the selected IP set to the Selected Objects list by clicking the  icon.

c Click **OK**.

5 To add IP addresses or domain names, type the address or name in the appropriate area.

6 Click **OK**.

Add Relay Agents

Add the Edge interfaces from which DHCP messages are to be relayed to the external DHP relay server(s).

Procedure

1 In the **DHCP Relay Agents** area, click the **Add** icon.

2 In **vNIC**, ensure that an internal vNIC is selected.

The **Gateway IP Address** displays the primary IP address of the selected vNic.

3 Click **OK**.

Configure DNS Servers

You can configure external DNS servers to which NSX Edge can relay name resolution requests from clients. NSX Edge will relay client application requests to the DNS servers to fully resolve a network name and cache the response from the servers.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click a NSX Edge.

4 Click the **Manage** tab and then click the **Settings** tab.

5 In the **DNS Configuration** panel, click **Change**.

6 Click **Enable DNS Service** to enable the DNS service.

7 Type IP addresses for both DNS servers.

8 Change the default cache size if required.

9 Click **Enable Logging** to log DNS traffic and select the log level.

Generated logs are sent to the syslog server.

10 Click **Ok**.

Service Composer 9

Service Composer helps you provision and assign network and security services to applications in a virtual infrastructure. You map these services to a security group, and the services are applied to the virtual machines in the security group.

Security Group

You begin by creating a security group to define assets that you want to protect. Security groups may be static (including specific virtual machines) or dynamic where membership may be defined in one or more of the following ways:

- vCenter containers (clusters, port groups, or datacenters)
- Security tags, IPset, MACset, or even other security groups. For example, you may include a criteria to add all members tagged with the specified security tag (such as AntiVirus.virusFound) to the security group.
- Directory Groups (if NSX Manager is registered with Active Directory)
- Regular expressions such as virtual machines with name *VM1*

Note that security group membership changes constantly. For example, a virtual machine tagged with the AntiVirus.virusFound tag is moved into the Quarantine security group. When the virus is cleaned and this tag is removed from the virtual machine, it again moves out of the Quarantine security group.

Security Policy

A security policy is a collection of the following service configurations.

Table 9-1. Security services contained in a security policy

Service	Description	Applies to
Firewall rules	Rules that define the traffic to be allowed to, from, or within the security group.	vNIC
Endpoint service	Data Security or third party solution provider services such as anti-virus or vulnerability management services.	virtual machines
Network introspection services	Services that monitor your network such as IPS.	virtual machines

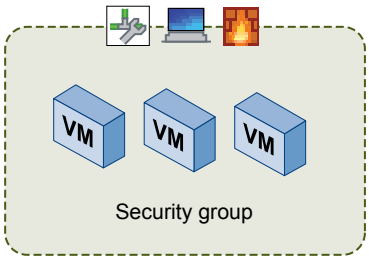
During service deployment in NSX, the third party vendor selects the service category for the service being deployed. A default service profile is created for each vendor template.

When third party vendor services are upgraded to NSX 6.1, default service profiles are created for the vendor templates being upgraded. Existing service policies that include Guest Introspection rules are updated to refer to the service profiles created during the upgrade.

Mapping Security Policy to Security Group

You map a security policy (say SP1) to a security group (say SG1). The services configured for SP1 are applied to all virtual machines that are members of SG1.

Figure 9-1. Service Composer overview



If a virtual machine belongs to more than one security group, the services that are applied to the virtual machine depends on the precedence of the security policy mapped to the security groups.

Service Composer profiles can be exported and imported as backups or for use in other environments. This approach to managing network and security services helps you with actionable and repeatable security policy management.

This chapter includes the following topics:

- "Using Service Composer," on page 116
- "Graphical View of Service Composer," on page 122
- "Export a Service Composer Configuration," on page 125
- "Import a Service Composer Configuration," on page 125
- "Working with Security Tags," on page 126
- "Viewing Effective Services," on page 127
- "Working with Security Policies," on page 129
- "Edit a Security Group," on page 130
- "Service Composer Scenarios," on page 130

Using Service Composer

Service Composer helps you consume security services with ease.

Let us walk through an example to show how Service Composer helps you protect your network end-to-end. Let us say you have the followings security policies defined in your environment:

- An initial state security policy that includes a vulnerability scanning service (InitStatePolicy)
- A remediation security policy that includes a network IPS service in addition to firewall rules and an anti-virus service (RemPolicy)

Ensure that the RemPolicy has higher weight (precedence) than InitStatePolicy.

You also have the followings security groups in place:

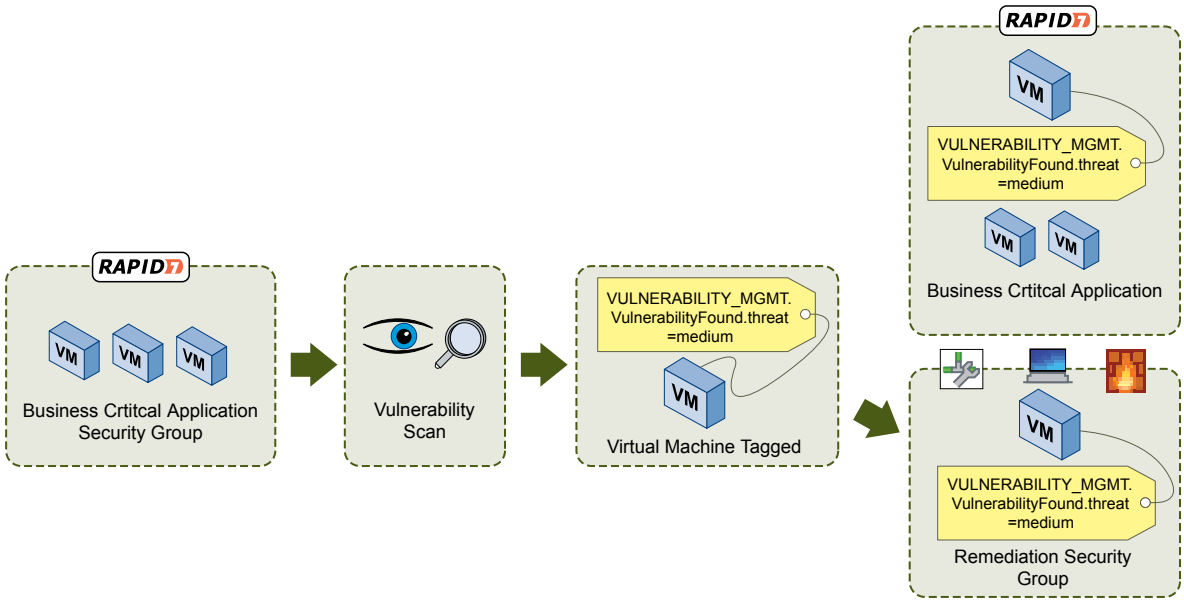
- An applications assets group that includes the business critical applications in your environment (AssetGroup)
- A remediation security group defined by a tag that indicates the virtual machine is vulnerable (`VULNERABILITY_MGMT.VulnerabilityFound.threat=medium`) named RemGroup

You now map the InitStatePolicy to AssetGroup to protect all business critical applications in your environment. You also map RemPolicy to RemGroup to protect vulnerable virtual machines.

When you initiate a vulnerability scan, all virtual machines in AssetGroup are scanned. If the scan identifies a virtual machine with a vulnerability, it applies the `VULNERABILITY_MGMT.VulnerabilityFound.threat=medium` tag to the virtual machine.

Service Composer instantly adds this tagged virtual machine to RemGroup, where a network IPS solution is already in place to protect this vulnerable virtual machine.

Figure 9-2. Service Composer in action



This topic will now take you through the steps required to consume the security services offered by Service Composer.

1 Create a Security Group in Service Composer on page 117

You create a security group at the NSX Manager level.

2 Create a Security Policy on page 119

A security policy is a set of Guest Introspection, firewall, and network introspection services that can be applied to a security group. The order in which security policies are displayed is determined by the weight associated with the policy. By default, a new policy is assigned the highest weight so that it is at the top of the table. However, you can modify the default suggested weight to change the order assigned to the new policy.

3 Map a Security Policy to a Security Group on page 122

You can apply a security policy to a security group to secure your virtual desktops, business critical applications, and the connections between them. You can also view a list of the services that were not applied and the reason they failed to apply.

Create a Security Group in Service Composer

You create a security group at the NSX Manager level.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Groups** tab and then click the **Add Security Group** icon.

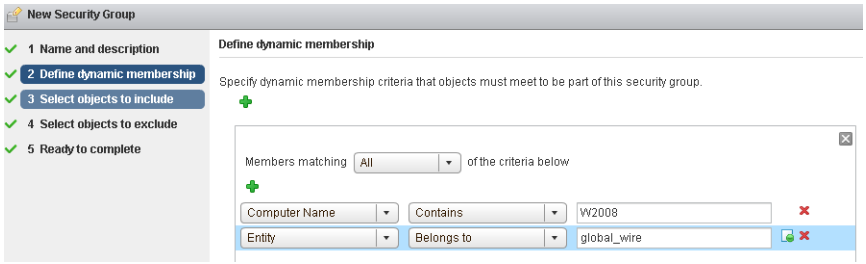
4 Type a name and description for the security group and click **Next**.

5 On the Dynamic Membership page, define the criteria that an object must meet for it to be added to the security group you are creating.

For example, you may include a criteria to add all members tagged with the specified security tag (such as AntiVirus.virusFound) to the security group. Security tags are case sensitive.

NOTE If you define a security group by virtual machines that have a certain security tag applied to them, you can create a dynamic or conditional workflow. The moment the tag is applied to a virtual machine, the virtual machine is automatically added to that security group.

Or you can add all virtual machines containing the name `W2008` AND virtual machines that are in the logical switch `global_wire` to the security group.



6 Click **Next**.

7 On the Select objects to include page, select the object type from the drop-down.

8 Double-click the object you want to add to the include list. You can include the following objects in a security group.

- Other security groups to nest within the security group you are creating.
- Cluster
- Logical switch
- Network
- Virtual App
- Datacenter
- IP sets
- AD groups

  NOTE The AD configuration for NSX security groups is different from the AD configuration for vSphere SSO. NSX AD group configuration is for end users accessing guest virtual machines while vSphere SSO is for administrators using vSphere and NSX.

- MAC Sets
- Security tag
- vNIC
- Virtual Machine

- Resource Pool
- Distributed Virtual Port Group

The objects selected here are always included in the security group regardless of whether or not they match the dynamic criteria.

When you add a resource to a security group, all associated resources are automatically added. For example, when you select a virtual machine, the associated vNIC is automatically added to the security group.

9 Click **Next** and double-click the objects that you want to exclude from the security group.

The objects selected here are always excluded from the security group even if they match the dynamic criteria or are selected in the include list .

10 Click **Finish**.

Membership of a security group is determined as follows:

{Expression result (derived from step 4) + Inclusions (specified in step 6} - Exclusion (specified in step 7)

which means that inclusion items are first added to the expression result. Exclusion items are then subtracted from the combined result.

Create a Security Policy

A security policy is a set of Guest Introspection, firewall, and network introspection services that can be applied to a security group. The order in which security policies are displayed is determined by the weight associated with the policy. By default, a new policy is assigned the highest weight so that it is at the top of the table. However, you can modify the default suggested weight to change the order assigned to the new policy.

Prerequisites

Ensure that:

- the required VMware built in services (such as Distributed Firewall, Data Security, and Guest Introspection) are installed.
- the required partner services have been registered with NSX Manager.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Policies** tab.

4 Click the **Create Security Policy** ( ) icon.

5 In the Add Security Policy dialog box, type a name for the security policy.

6 Type a description for the security policy.

NSX assigns a default weight (highest weight +1000) to the policy. For example, if the highest weight amongst the existing policy is 1200, the new policy is assigned a weight of 2200.

Security policies are applied according to their weight - a policy with the higher weight has precedence over a policy with a lower weight.

7 Select **Inherit security policy from specified policy** if you want the policy that you are creating to receive services from another security policy. Select the parent policy.

All services from the parent policy are inherited by the new policy.

8 Click **Next**.

9 In the Guest Introspection Services page, click the **Add Guest Introspection Service** ( ) icon.

a In the Add Guest Introspection Service dialog box, type a name and description for the service.

b Specify whether you want to apply the service or block it.

When you inherit a security policy, you may choose to block a service from the parent policy.

If you apply a service, you must select a service and service profile. If you block a service, you must select the type of service to block.

c If you chose to block the service, select the type of service.

If you select Data Security, you must have a data security policy in place. See Chapter 10, "Data Security," on page 135.

d If you chose to apply the Guest Introspection service, select the service name.

The default service profile for the selected service is displayed, which includes information about the service functionality types supported by the associated vendor template.

e In **State**, specify whether you want to enable the selected Guest Introspection service or disable it.

You can add Guest Introspection services as placeholders for services to be enabled at a later time. This is especially useful for cases where services need to be applied on-demand (for example, new applications).

f Select whether the Guest Introspection service is to be enforced (i.e. it cannot be overridden). If the selected service profile supports multiple service functionality types, then this is set to **Enforce** by default and cannot be changed.

If you enforce an Guest Introspection service in a security policy, other policies that inherit this security policy would require that this policy be applied before the other child policies. If this service is not enforced, an inheritance selection would add the parent policy after the child policies are applied.

g Click **OK**.

You can add additional Guest Introspection services by following the above steps. You can manage the Guest Introspection services through the icons above the service table.

You can export or copy the services on this page by clicking the  icon on the bottom right side of the Guest Introspection Services page.

10 Click **Next**.

11 On the Firewall page, click the **Add Firewall Rule** ( ) icon.

Here, you are defining firewall rules for the security groups(s) that this security policy will be applied to.

a Type a name and description for the firewall rule you are adding.

b Select **Allow** or **Block** to indicate whether the rule needs to allow or block traffic to the selected destination.

c Select the source for the rule. By default, the rule applies to traffic coming from the security groups to which this policy gets applied to. To change the default source, click **Change** and select the appropriate security groups.

d Select the destination for the rule.

NOTE Either the Source or Destination (or both) must be security groups to which this policy gets applied to.

Say you create a rule with the default Source, specify the Destination as Payroll, and select **Negate Destination**. You then apply this security policy to security group Engineering . This would result in Engineering being able to access everything except for the Payroll server.

e Select the services and/or service groups to which the rule applies to.

f Select **Enabled** or **Disabled** to specify the rule state.

g Select **Log** to log sessions matching this rule.

Enabling logging may affect performance.

h Click **OK**.

You can add additional firewall rules by following the above steps. You can manage the firewall rules through the icons above the firewall table.

You can export or copy the rules on this page by clicking the  icon on the bottom right side of the Firewall page.

The firewall rules you add here are displayed on the Firewall table. VMware recommends that you do not edit Service Composer rules in the firewall table. If you must do so for an emergency troubleshooting, you must re-synchronize Service Composer rules with firewall rules by selecting **Synchronize Firewall Rules** from the **Actions** menu in the Security Policies tab.

12 Click **Next**.

The Network Introspection Services page displays NetX services that you have integrated with your VMware virtual environment.

13 Click the **Add Network Introspection Service** () icon.

a In the Add Network Introspection Service dialog box, type a name and description for the service you are adding.

b Select whether or not to redirect to service.

c Select the service name and profile.

d Select the source and destination

e Select the network service that you want to add..

You can make additional selections based on the service you selected.

f Select whether to enable or disable the service.

g Select Log to log sessions matching this rule.

h Click **OK**.

You can add additional network introspection services by following the above steps. You can manage the network introspection services through the icons above the service table.

You can export or copy the services on this page by clicking the  icon on the bottom right side of the Network Introspection Service page.

14 Click **Finish**.

The security policy is added to the policies table. You can click the policy name and select the appropriate tab to view a summary of the services associated with the policy, view service errors, or edit a service.

What to do next

Map the security policy to a security group.

Map a Security Policy to a Security Group

You can apply a security policy to a security group to secure your virtual desktops, business critical applications, and the connections between them. You can also view a list of the services that were not applied and the reason they failed to apply.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Policy** tab.

4 Select a security policy and click the **Apply Security Policy** () icon.

5 Select the security group that you want to apply the policy to.

If you select a security group defined by virtual machines that have a certain security tag applied to them, you can create a dynamic or conditional workflow. The moment the tag is applied to a virtual machine, the virtual machine is automatically added to that security group.

6 Click the **Preview Service Status** icon to see the services that cannot be applied to the selected security group and the reason for the failure.

For example, the security group may include a virtual machine that belongs to a cluster on which one of the policy services has not been installed. You must install that service on the appropriate cluster for the security policy to work as intended.

7 Click **OK**.

Graphical View of Service Composer

Service Composer offers a canvas view displaying all security groups within the selected NSX Manager. The view also displays details such as members of each security group as well as the security policy applied on it.

This topic introduces Service Composer by walking you through a partially configured system so that you can visualize the mappings between security groups and security policy objects at a high level from the canvas view.

Procedure

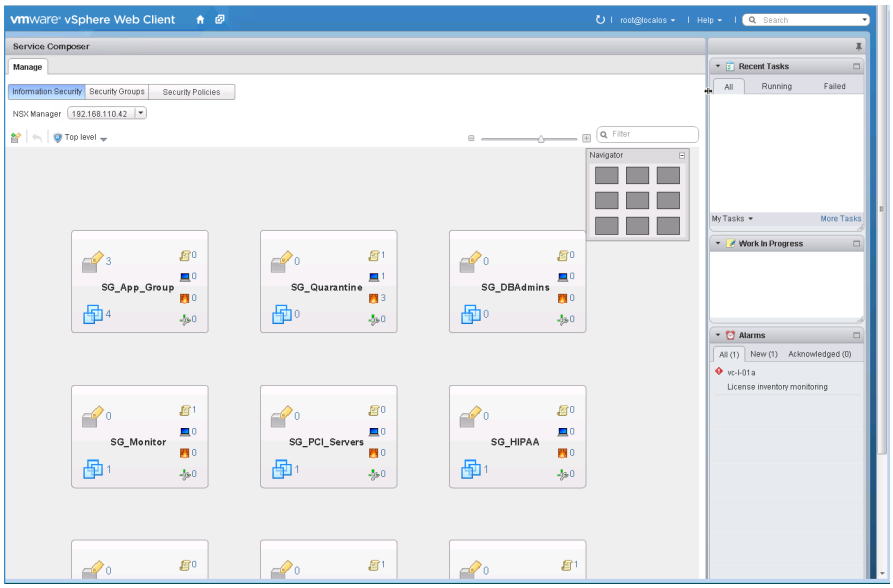
1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Canvas** tab.

All security groups within the selected NSX Manager (that are not contained within another security group) are displayed along with the policies applied on them. The **NSX Manager** drop-down lists all NSX Managers on which the currently logged in user has a role assigned.

Figure 9-3. Service Composer canvas top level view



Each rectangular box in the canvas represents a security group and the icons within the box represents security group members and details about the security policy mapped to the security group.

Figure 9-4. Security group

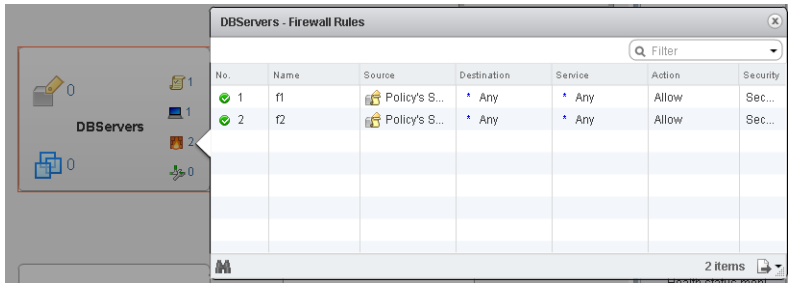
A number next to each icon indicates the number of instances - for example,  indicates that 1 security policy is mapped to that security group.

Icon	Click to display
	Security groups nested within the main security group.
	Virtual machines that are currently part of the main security group as well as nested security groups. Click the Errors tab to see virtual machines with service errors.
	Effective security policies mapped to the security group. ■ You can create a new security policy by clicking the Create **Security Policy** () icon. The newly created security policy object is automatically mapped to the security group. ■ Map additional security policies to the security group by clicking the **Apply Security Policy** () icon.
	Effective Endpoint services associated with the security policy mapped to the security group. Suppose you have two policies applied to a security group and both have the same category Endpoint service configured. The effective service count in this case will be 1 (since the second lower priority service is overridden). Endpoint service failures, if any, are indicated by the alert icon. Clicking the icon displays the error.

Icon	Click to display
	Effective firewall rules associated with the security policy mapped to the security group. Service failures, if any, are indicated by the alert icon. Clicking the icon displays the error.
	Effective network introspection services associated with the security policy mapped to the security group. Service failures, if any, are indicated by the alert icon. Clicking the icon displays the error.

Clicking an icon displays a dialog box with appropriate details.

Figure 9-5. Details displayed when you click an icon in the security group



You can search for security groups by name. For example, if you type PCI in the search field in the top right corner of the canvas view, only the security groups with PCI in their names are displayed.

To see the security group hierarchy, click the **Top Level** ( ) icon at the top left of the window and select the security group you want to display. If a security group contains nested security groups, click to display the nested groups. The top bar displays the name of the parent security group and the icons in the bar display the total number of security policies, endpoint services, firewall services, and network introspection services applicable to the parent group. You can navigate back up to the top level by clicking the **Go up one level** ( ) icon in the top left part of the window.

You can zoom in and out of the canvas view smoothly by moving the zoom slider on the top right corner of the window. The Navigator box shows a zoomed out view of the entire canvas. If the canvas is much bigger than what fits on your screen, it will show a box around the area that is actually visible and you can move it to change the section of the canvas that is being displayed.

What to do next

Now that we have seen how the mapping between security groups and security policies work, you can begin creating security policies to define the security services you want to apply to your security groups.

Map Security Group to Security Policy

You can map the selected security group to a security policy.

Procedure

1 Select the security policy that you want to apply to the security group.

2 To create a new policy, select New Security Group.

See "Create a Security Policy," on page 119.

3 Click **Save**.

Export a Service Composer Configuration

You can export a Service Composer configuration (along with the security groups to which the security policies are mapped) and save it to your desktop. The saved configuration can be used as a backup for situations where you may accidentally delete a policy configuration, or it can be exported for use in another NSX Manager environment.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Policies** tab.

4 Select the security policy that you want to export.

5 Click **Actions** and then click the **Export Service Configuration** icon.

6 Type a name and description for the configuration that you are exporting.

7 If desired, type a prefix to be added to the security policies and security groups that are being exported.

If you specify a prefix, it is added to the target security policy names thus ensuring that they have unique names.

8 Click **Next**.

9 In the Select security policies page, select the security policy that you want to export and click **Next**.

10 The Ready to complete page displays the security policies along with associated objects (security groups on which these have been applied, as well as Endpoint services, firewall rules, and network introspection services) to be exported.

11 Click **Finish**.

12 Select the directory on your computer where you want to download the exported blueprint and click **Save**.

The configuration file is saved at the specified location.

Import a Service Composer Configuration

You can import a saved Service Composer configuration (along with the security groups to which the security policies are mapped) either as a backup or to restore configuration on a different NSX Manager.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Policies** tab.

4 Click **Actions** and then click the **Import Service Configuration** icon.

5 Select the configuration file that you want to import.

6 If desired, type a suffix to be added to the security policies and security groups that are being imported.

If you specify a suffix, it is added to the security policy names being imported thus ensuring that they have unique names.

7 Click **Next**.

Service Composer verifies that all services referred to in the configuration are available in the destination environment. If not, the Manage Missing Services page is displayed, where you can map missing services to available target services.

The Ready to complete page displays the security policies along with associated objects (security groups on which these have been applied, as well as Endpoint services, firewall rules, and network introspection services) to be imported.

8 Click **Finish**.

The imported security policies are added to the top of the security policy table (above the existing policies) in the target NSX Manager. The original order of the imported policies is preserved.

Working with Security Tags

You can view security tags applied on a virtual machine or create a user defined security tag.

View Applied Security Tags

You can view the security tags applied to virtual machines in your environment.

Prerequisites

A data security or antivirus scan must have been run and a tag applied to the appropriate virtual machine.

NOTE Refer to the third party solution documentation for details of the tags applied by those solutions.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Security Tags** tab.

A list of tags applied in your environment is displayed along with details about the virtual machines to which those tags have been applied. Note down the exact tag name if you plan on adding a security group to include virtual machines with a specific tag.

5 Click the number in the **VM Count** column to view the virtual machines to which that tag in that row has been applied.

Add a Security Tag

You can manually add a security tag and apply it to a virtual machine. This is especially useful when you are using a non-NETX solution in your environment and hence, cannot register the solution tags with NSX Manager.

Prerequisites

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Security Tags** tab.

5 Click the **New Security Tag** ( ) icon.

6 Type a name and description for the tag and click **OK**.

Assign a Security Tag

In addition to creating a conditional workflow with a dynamic membership-based security tag, you can manually assign a security tag to a virtual machine.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Security Tags** tab.

5 Select a security tag and click the **Assign Security Tag** ( ) icon.

6 Select one or more virtual machines and click **OK**.

Edit a Security Tag

You can edit a user-defined security tag. If a security group is based on the tag you are editing, changes to the tag may affect security group membership.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Security Tags** tab.

5 Select a security tag and click the **Edit Security Tag** ( ) icon.

6 Make the appropriate changes and click **OK**.

Delete a Security Tag

You can delete a user-defined security tag. If a security group is based on the tag you are deleting, changes to the tag may affect security group membership.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Security Tags** tab.

5 Select a security tag and click the **Delete Security Tag** ( ) icon.

Viewing Effective Services

You can view the services that are effective on a security policy object or on a virtual machine.

View Effective Services on a Security Policy

You can view the services effective on a security policy, including those services inherited from a parent policy.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Policies** tab.

4 Click a security policy in the **Name** column.

5 Ensure that you are in the **Manage > Information Security** tab.

Each of the three tabs (**Endpoint Services**, **Firewall**, **Network Introspection Services**) displays the corresponding services for the security policy.

Services that are not effective are greyed out. The **Overridden** column displays the services that are actually applied on the security policy and the **Inherited from** column displays the security policy from which services are inherited.

View Service Failures for a Security Policy

You can see the services associated with a security policy that failed to apply to the security group(s) mapped to the policy.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Policies** tab.

4 Click a security policy in the **Name** column.

5 Ensure that you are in the **Monitor > Service Errors** tab.

Clicking the link in the **Status** column takes you to the Service Deployment page where you can correct service errors.

View Effective Services on a Virtual Machine

You can view the services effective on a virtual machine. If multiple security policies are getting applied on a virtual machine (i.e. a virtual machine is part of multiple security groups that have policies mapped to them), then this view lists all effective services from all these policies, in the order in which they get applied. The service status column displays the status for each service.

Procedure

1 Log in to the vSphere Web Client.

2 Click **vCenter** and then click **Virtual Machines**.

3 Click a virtual machine in the **Name** column.

4 Ensure that you are in the **Monitor > Service Composer** tab.

Working with Security Policies

A security policy is a group of network and security services.

The following network and security services can be grouped into a security policy:

- Endpoint services - data security, anti-virus, and vulnerability management
- Distributed Firewall rules
- Network introspection services - network IPS and network forensics

Manage Security Policy Priority

Security policies are applied according to their weight - a security policy with a higher weight has a higher priority. When you move a policy up or down in the table, its weight is adjusted accordingly.

Multiple security policies may be applied to a virtual machine either because the security group that contains the virtual machine is associated with multiple policies or because the virtual machine is part of multiple security groups associated with different policies. If there is a conflict between services grouped with each policy, the weight of the policy determines the services that will be applied to the virtual machine. For example, say policy 1 blocks internet access and has a weight value of 1000 while policy 2 allows internet access and has a weight value of 2000. In this particular case, policy 2 has a higher weight and hence the virtual machine will be allowed internet access.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Policies** tab.

4 Click the **Manage Precedence** () icon.

5 In the Manage Precedence dialog box, select the security policy that you want to change the precedence for and click the **Move Up** () or **Move Down** ()icon.

6 Click **OK**.

Edit a Security Policy

You can edit the name or description of a security policy, as well as the associated services and rules.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Policies** tab.

4 Select the security policy that you want to edit and click the **Edit Security Policy** () icon.

5 In the Edit Security Policy dialog box, make the appropriate changes and click **Finish**.

Delete a Security Policy

You can delete a security policy.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Policies** tab.

4 Select the security policy that you want to delete and click the **Delete Security Policy** ( ) icon.

Edit a Security Group

You can edit a security group.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Groups** tab.

4 Select the security group you want to edit and click the **Edit Security Group** icon.

5 Make the appropriate changes and click **OK**.

Service Composer Scenarios

This section illustrates some hypothetical scenarios for Service Composer. It is assumed that the Security Administrator role has been created and assigned to the administrator in each use case.

Quarantining Infected Machines Scenario

Service Composer can identify infected systems on your network with 3rd party antivirus solutions and quarantine them to prevent further outbreaks.

Our sample scenario shows how you can protect your desktops end to end.

Figure 9-6. Configuring Service Composer

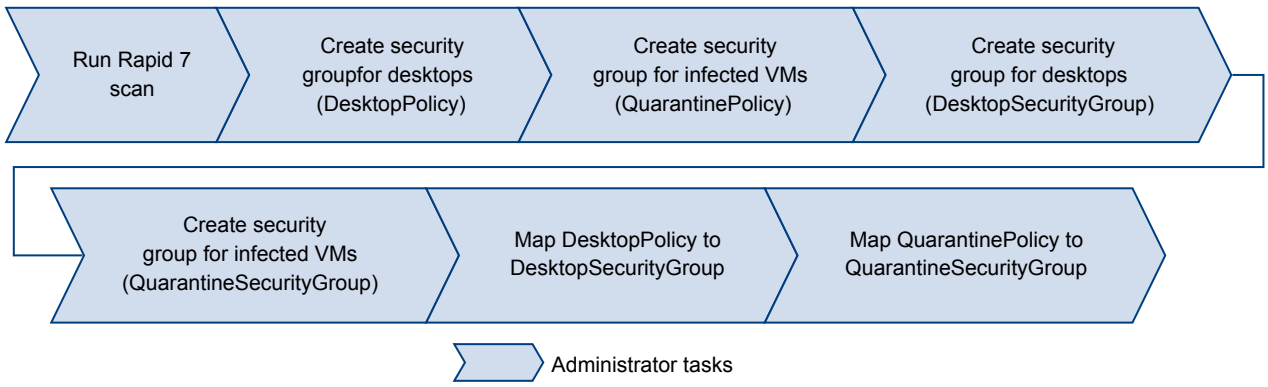
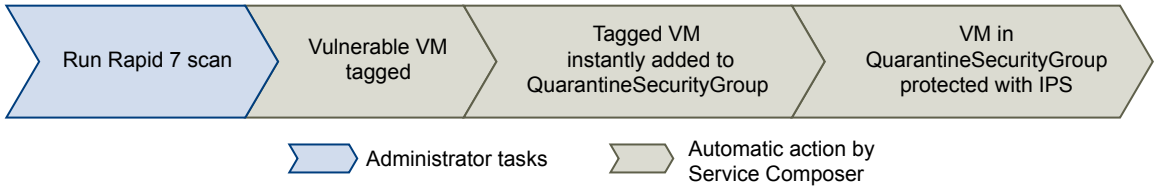


Figure 9-7. Service Composer Conditional Workflow



Prerequisites

We are aware that Symantec tags infected virtual machine with the **`AntiVirus.virusFound`** tag.

Procedure

1 Install, register, and deploy the Symantec Antimalware solution.

2 Create a security policy for your desktops.

a Click the **Security Policies** tab and click the **Add Security Policy** icon.

b In **Name**, type **`DesktopPolicy`**.

c In **Description**, type **`Antivirus scan for all desktops`**.

d Change the weight to 51000. The policy precedence is set very high so as to ensure that it is enforced above all other policies.

e Click **Next**.

f On the Add Endpoint Service page, click  and fill in the following values.

Option	Value
Action	Do not modify the default value
Service Type	Anti Virus
Service Name	Symantec Antimalware
Service Configuration	Silver
State	Do not modify the default value
Enforce	Do not modify the default value
Name	Desktop AV
Description	Mandatory policy to be applied on all desktops

g Click **OK**.

h Do not add any firewall or network introspection services and click **Finish**.

3 Create a security policy for infected virtual machines.

a Click the **Security Policies** tab and click the **Add Security Policy** icon.

b In Name, type **`QuarantinePolicy`**.

c In Description, type **`Policy to be applied to all infected systems.`**.

d Do not change the default weight.

e Click **Next**.

f On the Add Endpoint Service page, do not do anything and click **Next**.

g In Firewall, add three rules - one rule to block all outgoing traffic, the next rule to block all traffic with groups, and the last rule to allow incoming traffic only from remediation tools.

h Do not add any network introspection services and click **Finish**.

4 Move **`QuarantinePolicy`** to the top of the security policy table to ensure that it is enforced before all other policies.

a Click the **Manage Priority** icon.

b Select **`QuarantinePolicy`** and click the **Move Up** icon.

5 Create a security group for all desktops in your environment.

a Log in to the vSphere Web Client.

b Click **Networking & Security** and then click **Service Composer**.

c Click the **Security Groups** tab and click the **Add Security Group** icon.

d In Name, type **`DesktopSecurityGroup`**.

e In Description, type **`All desktops`**.

f Click **Next** on the next couple of pages.

g Review your selections on the Ready to Complete page and click **Finish**.

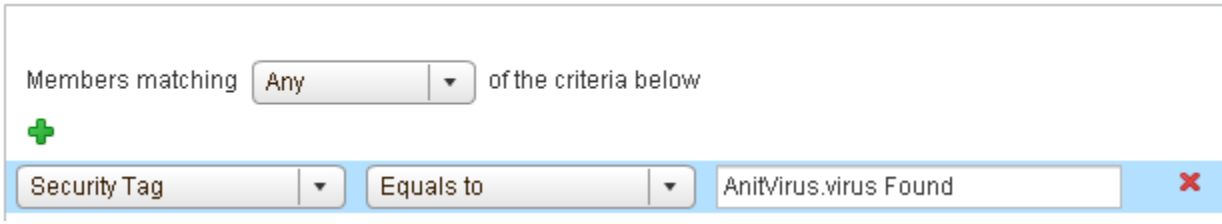
6 Create a Quarantine security group where the infected virtual machines are to be placed.

a Click the **Security Groups** tab and click the **Add Security Group** icon.

b In **Name**, type **`QuarantineSecurityGroup`**.

c In **Description**, type
`Dynamic group membership based on infected VMs identified by the antivirus scan`.

d On the Define membership Criteria page click and add the following criteria.



e Do not do anything on the Select objects to include or Select objects to exclude pages and click **Next**.

f Review your selections on the Ready to Complete page and click **Finish**.

7 Map the **`DesktopPolicy`** policy to the **`DesktopSecurityGroup`** security group.

a On the Security Policies tab, ensure that the **`DesktopPolicy`** policy is selected.

b Click the **Apply Security Policy** ( ) icon and select the SG_Desktops group.

c Click **OK**.

This mapping ensures that all desktops (part of the **`DesktopSecurityGroup`**) are scanned when an antivirus scan is triggered.

8 Navigate to the canvas view to confirm that **QuarantineSecurityGroup** does not include any virtual machines yet.

   a Click the **Information Security** tab.

   b Confirm that there are 0 virtual machines in the group ()

9 Map **QuarantinePolicy** to **QuarantineSecurityGroup**.

   This mapping ensures that no traffic flows to the infected systems.

10 From the Symantec Antimalware console, trigger a scan on your network.

   The scan discovers infected virtual machine and tags them with the security tag **AntiVirus.virusFound**. The tagged virtual machines are instantly added to **QuarantineSecurityGroup**. The **QuarantinePolicy** allows no traffic to and from the infected systems.

Backing up Security Configurations

Service Composer can be very effectively used to back up your security configurations and restore them at a later time.

Procedure

1 Install, register, and deploy the Rapid 7 Vulnerability Management solution.

2 Create a security group for the first tier of the Share Point application - web servers.

   a Log in to the vSphere Web Client.

   b Click **Networking & Security** and then click **Service Composer**.

   c Click the **Security Groups** tab and click the **Add Security Group** icon.

   d In **Name**, type **SG_Web**.

   e In **Description**, type **Security group for application tier**.

   f Do not do anything on the Define membership Criteria page and click **Next**.

   g On the Select objects to include page, select the web server virtual machines.

   h Do not do anything on the Select objects to exclude page and click **Next**.

   i Review your selections on the Ready to Complete page and click **Finish**.

3 Now create a security group for your database and share point servers and name them **SG_Database**, and **SG_Server_SharePoint** respectively. Include the appropriate objects in each group.

4 Create a top level security group for your application tiers and name it **SG_App_Group**. Add SG_Web, SG_Database, and SG_Server_SharePoint to this group.

5 Create a security policy for your web servers.

   a Click the Security Policies tab and click the Add Security Policy icon.

   b In Name, type **SP_App**.

   c In Description, type **SP for application web servers**.

   d Change the weight to 50000. The policy precedence is set very high so as to ensure that it is enforced above most other policies (with the exception of quarantine).

   e Click Next.

f On the Endpoint Services page, click and fill in the following values.

Option	Value
Action	Do not modify the default value
Service Type	Vulnerability Management
Service Name	Rapid 7
Service Configuration	Silver
State	Do not modify the default value
Enforce	Do not modify the default value

g Do not add any firewall or network introspection services and click **Finish**.

6 Map SP_App to SG_App_Group.

7 Navigate to the canvas view to confirm that the SP_App has been mapped to SG_App_Group.

a Click the Information Security tab.

b Click the number next to the icon to see that the SP_App is mapped.

8 Export the SP_App policy.

a Click the Security Policies tab and then click the **Export Blueprint** ( ) icon.

b In **Name**, type **`Template_ App_`** and in **Prefix**, type **`FromAppArchitect`**.

c Click Next.

d Select the SP_App policy and click Next.

e Review your selections and click Finish.

f Select the directory on your computer where you want to download the exported file and click Save.

The security policy as well as all the security groups to which this policy has been applied (in our case, the Application security group as well as the three security groups nested within it) are exported.

9 In order to demonstrate how the exported policy works, delete the SP_App policy.

10 Now we will restore the Template_ App_ DevTest policy that we exported in step 7.

a Click **Actions** and then click the **Import Service Configuration** icon.

b Select the **`FromAppArtchitect_Template_App`** file from your desktop (you saved it in step 7).

c Click **Next**.

d The Ready to complete page displays the security policies along with associated objects (security groups on which these have been applied, as well as Endpoint services, firewall rules, and network introspection services) to be imported.

e Click **Finish**.

The configuration and associated objects are imported to the vCenter inventory and are visible in the canvas view.

10 Data Security

NSX Data Security provides visibility into sensitive data stored within your organization's virtualized and cloud environments. Based on the violations reported by NSX Data Security, you can ensure that sensitive data is adequately protected and assess compliance with regulations around the world.

To begin using NSX Data Security, you create a policy that defines the regulations that apply to data security in your organization and specifies the areas of your environment and files to be scanned. A regulation is composed of content blades, which identify the sensitive content to be detected. NSX supports PCI, PHI, and PII related regulations only.

When you start a Data Security scan, NSX analyzes the data on the virtual machines in your vSphere inventory and reports the number of violations detected and the files that violated your policy.

This chapter includes the following topics:

- "NSX Data Security User Roles," on page 135
- "Defining a Data Security Policy," on page 135
- "Running a Data Security Scan," on page 137
- "Viewing and Downloading Reports," on page 138
- "Creating Regular Expressions," on page 138

NSX Data Security User Roles

A user's role determines the actions that the user can perform.

Role	Actions Allowed
Security Administrator	Create and publish policies and view violation reports. Cannot start or stop a data security scan.
NSX Administrator	Start and stop data security scans.
Auditor	View configured policies and violation reports.

Defining a Data Security Policy

To detect sensitive data in your environment, you must create a data security policy. You must be a Security Administrator to create policies.

To define a policy, you must specify the following:

1 Regulations

A regulation is a data privacy law for protecting PCI (Payment Card Industry), PHI (Protected Health Information) and PII (Personally Identifiable Information) information. You can select the regulations that your company needs to comply to. When you run a scan, Data Security identifies data that violates the regulations in your policy and is sensitive for your organization.

2 File filters

You can create filters to limit the data being scanned and exclude file types unlikely to contain sensitive data from the scan.

Select Regulations

After you select the regulations that you want your company data to comply with, NSX can identify files that contain information in violation of these regulations.

Prerequisites

You must have the Security Administrator role.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking and Security** and then click **Data Security**.

3 Click the **Manage** tab.

4 Click **Edit** and click **All** to display all available regulations.

5 Select the regulations for which you want to detect compliance.

NOTE For information on available regulations, see Chapter 16, "Data Security Regulations," on page 219.

6 Click **Next**.

7 Certain regulations require additional information for NSX Data Security to recognize sensitive data. If you selected a regulation that monitors Group Insurance Numbers, Patient Identification Numbers, Medical Record Numbers, Health Plan Beneficiary Numbers, US Bank Account Numbers, Custom Accounts, or Student identification numbers, specify a regular expression pattern for identifying that data.

NOTE Check the accuracy of the regular expression. Specifying incorrect regular expressions can slow down the discovery process. For more information on regular expressions, see "Creating Regular Expressions," on page 138.

8 Click **Finish.**

9 Click **Publish Changes** to apply the policy.

Specify File Filters

You can restrict the files that you want to monitor based on size, last modified date, or file extensions.

Prerequisites

You must have been assigned the Security Administrator role.

Procedure

1 In the **Manage** tab of the Data Security panel, click **Edit** next to **Files to scan**.

2 You can either monitor all files on the virtual machines in your inventory, or select the restrictions you want to apply.

Option	Description
Monitor all files on the guest virtual machines	NSX Data Security scans all files.
Monitor only the files that match the following conditions	Select the following options as appropriate. ■ **Size** indicates that NSX Data Security should only scan files less than the specified size. ■ **Last Modified Date** indicates that NSX Data Security should scan only files modified between the specified dates. ■ **Types:** Select **Only files with the following extensions** to enter the file types to scan. Select **All files, except those with extensions** to enter the file types to exclude from the scan.

For information on file formats that NSX Data Security can detect, see Chapter 18, "File Formats Supported by Data Security," on page 281.

3 Click **Save.**

4 Click **Publish Changes** to apply the policy.

Running a Data Security Scan

Running a data security scan identifies data in your virtual environment that violates your policy.

Prerequisites

You must be a NSX Administrator to start, pause, or stop a data security scan.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking and Security** and then click **Data Security**.

3 Click the **Manage** tab.

4 Click **Start** next to Scanning.

NOTE If a virtual machine is powered off, it will not be scanned until it is powered on.

If a scan is in progress, the available options are **Pause** and **Stop**.

If Data Security is part of a Service Composer policy, virtual machines in the security group mapped to that Service Composer policy are scanned once during a scan. If the policy is edited and published while a scan is running, the scan restarts. This rescan ensures that all virtual machines comply with the edited policy. A rescan is triggered by publishing an edited policy, not by data updates on your virtual machines.

If a virtual machine is moved to an excluded cluster or resource pool while the data security scan is in progress, the files on that virtual machine are not scanned. In case a virtual machine is moved by vMotion to another host, the scan continues on the second host. Files that were scanned while the virtual machine was on the previous host are not rescanned.

When the Data Security engine starts scanning a virtual machine, it records the scan start time. When the scan ends, it records the end of the scan. You can view the scan start and end time for a cluster, host, or virtual machine on the **Tasks and Events** tab.

NSX Data Security throttles the number of virtual machines concurrently scanned on a host to minimize impact on performance. VMware recommends that you pause the scan during normal business hours to avoid any performance overhead.

Viewing and Downloading Reports

When you start a security scan, NSX displays the start and end time of each scan, the number of virtual machines scanned, and the number of violations detected.

Prerequisites

You have the Security Administrator or Auditor role.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking and Security** and then click **Data Security**.

3 Click the **Reports** tab.

4 Specify the report for Violation counts or for Violating files.

Creating Regular Expressions

A regular expression is a pattern that describes a certain sequence of text characters, otherwise known as strings. You use regular expressions to search for, or match, specific strings or classes of strings in a body of text.

Using a regular expression is like performing a wildcard search, but regular expressions are far more powerful. Regular expressions can be very simple or very complex. An example of a simple regular expression is *cat*.

This finds the first instance of the letter sequence cat in any body of text that you apply it to. If you want to make sure it only finds the word *cat*, and not other strings like *cats* or *hepcat*, you could use this slightly more complex regular expression: *\bcat\b*.

This expression includes special characters that ensure a match occurs only if there are word breaks on both sides of the *cat* sequence. As another example, to perform a near equivalent to the typical wildcard search string *c+t*, you could use this regular expression: *\bc\w+t\b*.

This means find a word boundary (\b) followed by a *c*, followed by one or more non-whitespace characters, non-punctuation characters (\w+), followed by a *t*, followed by a word boundary (\b). This expression finds *cot*, *cat*, *croat*, but not *crate*.

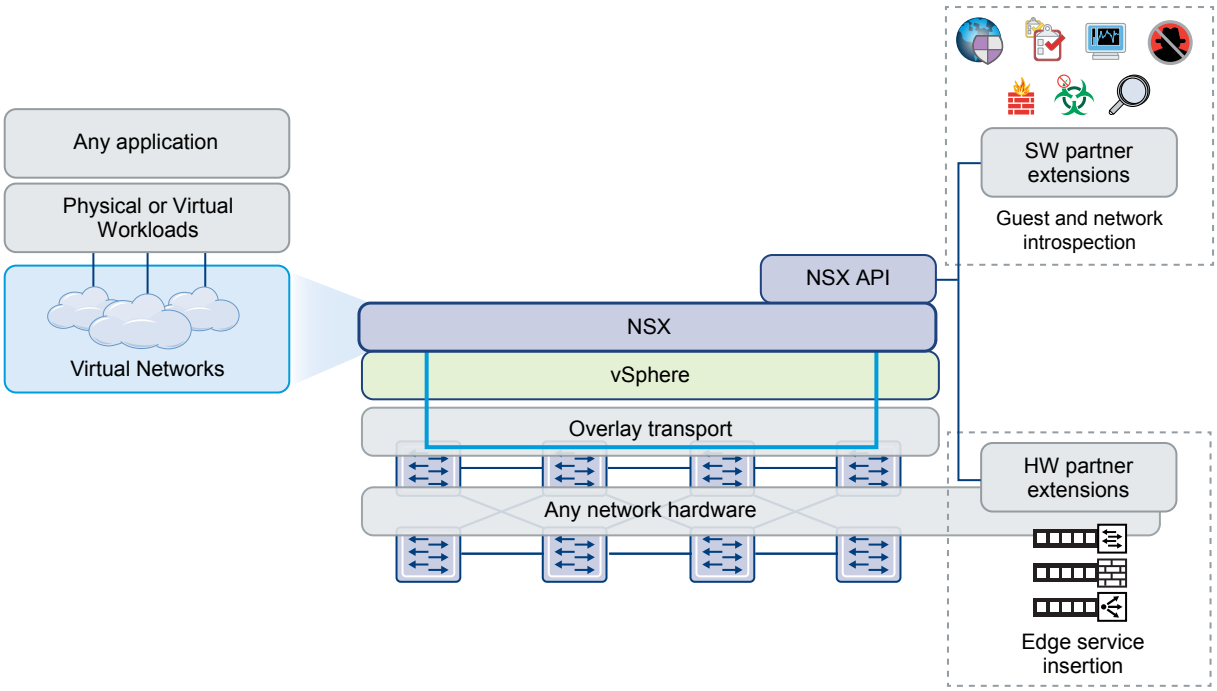
Expressions can be very complex. The following expression finds any valid email address.

\b[A-Za-z0-9._%-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}\b

For more information on creating regular expressions, see http://userguide.icu-project.org/strings/regexp.

11 Network Extensibility

Datacenter networks typically involve a wide range of network services, including switching, routing, firewalling, load balancing, and so on.. In most cases, these services are delivered by different vendors. In the physical world, connecting these services in the network is a complicated exercise of racking and stacking physical network devices, establishing physical connectivity, and managing these services separately. NSX simplifies the experience of connecting the right services in the right traffic paths and can help you build complex networks within a single ESX Server host or across multiple ESX server hosts for production, testing, or development purposes.



There are various deployment methods for inserting third party services into NSX.

This chapter includes the following topics:

- "Distributed Service Insertion," on page 140
- "Edge-Based Service Insertion," on page 140
- "Integrating Third Party Services," on page 140
- "Consuming Vendor Services through Service Composer," on page 140
- "Redirecting Traffic to a Vendor Solution through Logical Firewall," on page 141

- "Using a Partner Load Balancer," on page 141

Distributed Service Insertion

In distributed service insertion, a single host has all service modules, kernel modules, and virtual machine implementations on a single physical machine. All components of the system interact with components within the physical host. This allows for faster module-to-module communication and compact deployment models. The same configuration can be replicated on physical systems in the network for scalability, while control and data plane traffic to and from the service modules to the vmkernel stay on the same physical system. During vMotion of the protected virtual machines, the partner security machine moves the virtual machine state from the source to the destination host.

Vendor solutions that make use of this type of service insertion include Intrusion Prevention Service (IPS)/Intrusion Detection Service (IDS), Firewall, Anti Virus, File Identity Monitoring (FIM), and Vulnerability Management.

Edge-Based Service Insertion

NSX Edge is deployed as a virtual machine in the Edge Services Cluster along with other network services. NSX Edge has the capability to redirect specific traffic to 3rd-party network services..

Vendor solutions that make use of this type of service insertion include ADC/Load Balancer devices.

Integrating Third Party Services

This is a generic high-level workflow for inserting a third-party service into the NSX platform.

Procedure

1 Register the third-party service with NSX Manager on the vendor's console.

You need NSX login credentials to register the service. For more information, refer to the vendor documentation.

2 Deploy the service in NSX. See Deploy a Partner Service.

Once deployed, the third-party service is displayed in the NSX Service Definitions window and is ready to be used. The procedure for using the service in NSX depends on the type of service inserted.

For example, you can enable a host-based firewall service by creating a security policy in Service Composer or creating a firewall rule to redirect traffic to the service. See "Consuming Vendor Services through Service Composer," on page 140 or "Redirecting Traffic to a Vendor Solution through Logical Firewall," on page 141. For information on using an Edge based service, see "Using a Partner Load Balancer," on page 141.

Consuming Vendor Services through Service Composer

Third-party vendor services include traffic redirection, load balancer, and guest security services such as data loss prevention, anti virus, and so on. Service Composer enables you to apply these services to a set of vCenter objects.

A security group is a set of vCenter objects such as clusters, virtual machines, vNICs, and logical switches. A security policy is a set of Guest Introspection services, firewall rules, and network introspection services.

When you map a security policy to a security group, redirection rules are created on the appropriate third-party vendor service profile. As traffic flows from virtual machines belonging to that security group, it is redirected to registered third-party vendor services that determine how to process that traffic. For more information on Service Composer, see "Using Service Composer," on page 116.

Redirecting Traffic to a Vendor Solution through Logical Firewall

You can add firewall rules to redirect traffic to registered vendor solutions. Redirected traffic is then processed by the vendor service.

Prerequisites

- The third party service must be registered with NSX Manager, and the service must be deployed in NSX.
- If the default firewall rule action is set to Block, you must add a rule to allow the traffic to be redirected.

Procedure

1. In the vSphere Web Client, navigate to **Networking & Security > Firewall**.
2. Click the **Partner security services** tab.
3. In the section to which you want to add a rule, click the **Add rule** ( ) icon.

   A new any any allow rule is added at the top of the section.
4. Point to the **Name** cell of the new rule, click , and type a name for the rule.
5. Specify the **Source**, **Destination**, and **Service** for the rule. For more information, see "Add a Firewall Rule," on page 43
6. Point to the **Action** cell of the new rule, click , and select the appropriate service profile from the **Redirect To** .
7. Indicate whether the redirected traffic is to be logged and type comments, if any.
8. Click **OK**.

   The selected service profile is displayed as a link in the **Action** column. Clicking the service profile link displays the service profile bindings.
9. Click **Publish Changes**.

Using a Partner Load Balancer

You can use a third-party load balancer to balance the traffic for a specific NSX Edge.

Prerequisites

The third-party load balancer must be registered with NSX Manager, and it must be deployed in NSX.

Procedure

1. In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.
2. Double-click an NSX Edge.
3. Click **Manage** and then click the **Load Balancer** tab.
4. Click **Edit** next to Load balancer global configuration.
5. Select **Enable Load Balancer** and **Enable Service Insertion**.
6. In **Service Definition**, select the appropriate partner load balancer.
7. In **Service Configuration**, select the appropriate service configuration.

8 Complete the remaining fields and set up the load balancer by adding a service monitor, server pool, application profile, application rules, and a virtual server. When adding a virtual server, select the template provided by the vendor. For more information, see "Set Up Load Balancing," on page 97.

Traffic for the specified Edge is load balanced by the third party vendor's management console.

12 User Management

In many organizations, networking and security operations are handled by different teams or members. Such organizations may require a way to limit certain operations to specific users. This topic describes the options provided by NSX to configure such access control.

NSX also supports Single Sign On (SSO), which enables NSX to authenticate users from other identity services such as Active Directory, NIS, and LDAP.

User management in the vSphere Web Client is separate from user management in the CLI of any NSX component.

This chapter includes the following topics:

- "Configure Single Sign On," on page 143
- "Managing User Rights," on page 144
- "Managing the Default User Account," on page 145
- "Assign a Role to a vCenter User," on page 145
- "Edit a User Account," on page 147
- "Change a User Role," on page 148
- "Disable or Enable a User Account," on page 148
- "Delete a User Account," on page 148

Configure Single Sign On

Integrating the single sign on (SSO) service with NSX improves the security of user authentication for vCenter users and enables NSX to authenticate users from other identity services such as AD, NIS, and LDAP.

With SSO, NSX supports authentication using authenticated Security Assertion Markup Language (SAML) tokens from a trusted source via REST API calls. NSX Manager can also acquire authentication SAML tokens for use with other VMware solutions.

Prerequisites

- SSO service must be installed on the vCenter Server.
- NTP server must be specified so that the SSO server time and NSX Manager time is in sync. See "Edit the NSX Manager Date and Time," on page 161.

Procedure

1 Log in to the NSX Manager virtual appliance.

2 Under Appliance Management, click **Manage Settings**.

3 Click **NSX Management Service**.

4 Click **Edit** next to **Lookup Service**.

5 Type the name or IP address of the host that has the lookup service.

6 Change the port number if required. The default port is 7444.

The Lookup Service URL is displayed based on the specified host and port.

7 Type the vCenter administrator user name and password (for example, administrator@vsphere.local).

This enables NSX Manager to register itself with the Security Token Service server.

8 Click **OK**.

Confirm that the Lookup Service status is Connected.

What to do next

Assign a role to the SSO user.

Managing User Rights

A user's role defines the actions the user is allowed to perform on a given resource. The role determines the user's authorized activities on the given resource, ensuring that a user has access only to the functions necessary to complete applicable operations. This allows domain control over specific resources, or system-wide control if your right has no restrictions.

The following rules are enforced:

- A user can have only one role.
- You cannot add a role to a user or remove an assigned role from a user. You can, however, change the assigned role for a user.

Table 12-1. NSX Manager User Roles

Right	Permissions
Enterprise Administrator	NSX operations and security.
NSX Administrator	NSX operations only: for example, install virtual appliances, configure port groups.
Security Administrator	NSX security only: for example, define data security policies, create port groups, create reports for NSX modules.
Auditor	Read only.

The scope of a role determines what resources a particular user can view. The following scopes are available for NSX users.

Table 12-2. NSX Manager User Scope

Scope	Description
No restriction	Access to entire NSX system.
Limit access scope	Access to a specified Edge.

The Enterprise Administrator and NSX Administrator roles can be assigned only to vCenter users, and their access scope is global (no restrictions).

Managing the Default User Account

The NSX Manager user interface includes a user account, which has access rights to all resources. You cannot edit the rights of or delete this user. The default user name is **admin** and the default password is **default** or the password you specified during NSX Manager installation.

You can manage NSX Manager appliance **admin** user only through CLI commands.

Assign a Role to a vCenter User

When you assign a role to an SSO user, vCenter authenticates the user with the identity service configured on the SSO server. If the SSO server is not configured or is not available, the user is authenticated either locally or with Active Directory based on vCenter configuration.

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the Name column and then click the **Manage** tab.

4 Click **Users**.

5 Click **Add**.

The Assign Role window opens.

6 Click **Specify a vCenter user** or **Specify a vCenter group**.

7 Type the vCenter **User** or **Group** name for the user.

NOTE If the vCenter user is from a domain (such as a SSO user), you must enter a fully qualified windows domain path. This will allow the default NSX Manager user (admin) as well as the SSO default user (admin) to login to NSX Manager. This user name is for logging in to the NSX Manager user interface, and cannot be used to access NSX Manager CLIs.

---

8 Click **Next**.

9 Select the role for the user and click **Next**. For more information on the available roles, see "Managing User Rights," on page 144.

10 Select the scope for the user and click **Finish**.

The user account appears in the Users table.

Understanding Group-Based Role Assignments

Organizations create user groups for proper user management. After integration with SSO, NSX Manager can get the details of groups to which a user belongs. Instead of assigning roles to individual users who may belong to the same group, NSX Manager assigns roles to groups. The following scenarios illustrate how NSX Manager assigns roles.

Example: Role-Based Access Control Scenario

This scenario provides an IT network engineer (Sally Moore) access to NSX components in the following environment.

AD domain: corp.local, vCenter group: neteng@corp.local, user name: smoore@corp.local

Prerequisites: vCenter Server has been registered with NSX Manager, and SSO has been configured.

1 Assign a role to Sally.

a Log in to the vSphere Web Client.

b Click **Networking & Security** and then click **NSX Managers**.

c Click an NSX Manager in the Name column and then click the **Manage** tab.

d Click **Users** and then click **Add**.

The Assign Role window opens.

e Click **Specify a vCenter group** and type `neteng@corp.local` in **Group**.

f Click **Next**.

g In Select Roles, click **NSX Administrator** and then click **Next**.

h In Limit Scope, select **No restriction** and click **Finish**.

2 Grant Sally permission to the datacenter.

a Click the Home icon and then click **vCenter Home > Datacenters**.

b Select a datacenter and click **Actions > All vCenter Actions > Add Permission**.

c Click **Add** and select the domain CORP.

d In **Users and Groups**, select **Show Groups First**.

e Select NetEng and click **OK**.

f In **Assigned Role**, select **Read-only** and un-select **Propagate to children** and click **OK**.

3 Log out of vSphere Web Client and log back in as smoore@corp.local.

Sally can perform NSX operations only. For example, install virtual appliances, create logical switches, and so on..

Example: Inherit PermissionsThrough aUser-Group MembershipScenario

Group option	Value
Name	G1
Role assigned	Auditor (Read only)
Resources	Global root

User option	Value
Name	John
Belongs to group	G1
Role assigned	None

John belongs to group G1, which has been assigned the auditor role. John inherits the group role and resource permissions.

Example: User Member of Multiple Groups Scenario

Group option	Value
Name	G1
Role assigned	Auditor (Read only)
Resources	Global root

Group option	Value
Name	G2
Role assigned	Security Administrator (Read and Write)
Resources	Datacenter1

User option	Value
Name	Joseph
Belongs to group	G1, G2
Role assigned	None

Joseph belongs to groups G1 and G2 and inherits a combination of the rights and permissions of the Auditor and Security Administrator roles. For example, John has the following permissions:

- Read, write (Security Administrator role) for Datacenter1
- Read only (Auditor) for global root

Example: User Member of Multiple Roles Scenario

Group option	Value
Name	G1
Role assigned	Enterprise Administrator
Resources	Global root

User option	Value
Name	Bob
Belongs to group	G1
Role assigned	Security Administrator (Read and Write)
Resources	Datacenter1

Bob has been assigned the Security Administrator role, so he does not inherit the group role permissions. Bob has the following permissions

- Read, write (Security Administrator role) for Datacenter1 and its child resources
- Enterprise Administrator role on Datacenter1

Edit a User Account

You can edit a user account to change the role or scope. You cannot edit the **`admin`** account.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the Name column and then click the **Manage** tab.

4 Click **Users**.

5 Select the user you want to edit.

6 Click **Edit**.

7 Make changes as necessary.

8 Click **Finish** to save your changes.

Change a User Role

You can change the role assignment for all users, except for the **admin** user.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the Name column and then click the **Manage** tab.

4 Click **Users**.

5 Select the user you want to change the role for.

6 Click **Change Role**.

7 Make changes as necessary.

8 Click **Finish** to save your changes.

Disable or Enable a User Account

You can disable a user account to prevent that user from logging in to the NSX Manager. You cannot disable the **admin** user or a user who is currently logged into the NSX Manager.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the Name column and then click the **Manage** tab.

4 Click **Users**.

5 Select a user account.

6 Click the **Enable** or **Disable** icon.

Delete a User Account

You can delete any created user account. You cannot delete the **admin** account. Audit records for deleted users are maintained in the database and can be referenced in an Audit Log report.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the Name column and then click the **Manage** tab.

4 Click **Users**.

5 Select a user account.

6 Click **Delete**.

7 Click **OK** to confirm deletion.

If you delete a vCenter user account, only the role assignment for NSX Manager is deleted. The user account on vCenter is not deleted.

Network and Security Objects 13

This section describes custom network and security containers .

This chapter includes the following topics:

- "Working with IP Address Groups," on page 149
- "Working with MAC Address Groups," on page 150
- "Working with IP Pools," on page 151
- "Working with Security Groups," on page 152
- "Working with Services and Service Groups," on page 154

Working with IP Address Groups

Create an IP Address Group

You can create an IP address group and then add this group as the source or destination in a firewall rule. Such a rule can help protect physical machines from virtual machines or vice versa.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **IP Sets**.

5 Click the **Add** ( ) icon and select **IP Addresses**.

The Add IP Addresses window opens.

6 Type a name for the address group.

7 (Optional) Type a description for the address group.

8 Type the IP addresses to be included in the group.

9 Click **OK**.

Edit an IP Address Group

Prerequisites

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then **click IP Sets**.

5 Select the group that you want to edit and click the **Edit** ( ) icon.

6 In the Edit IP Addresses dialog box, make the appropriate changes.

7 Click **OK**.

Delete an IP Address Group

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **IP Sets**.

5 Select the group that you want to delete and click the **Delete** ( ) icon.

Working with MAC Address Groups

Create a MAC Address Group

You can create a MAC address group consisting of a range of MAC addresses and then add this group as the source or destination in a Distributed Firewall rule. Such a rule can help protect physical machines from virtual machines or vice versa.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **MAC Sets**.

5 Click the **Add** ( ) icon.

6 Type a name and description for the address group.

7 Type the MAC addresses to be included in the group.

8 Click **OK**.

Edit a MAC Address Group

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **MAC Sets**.

5 Select the group that you want to edit and click the **Edit** ( ) icon.

6 In the Edit MAC Addresses dialog box, make the appropriate changes.

7 Click **OK**.

Delete a MAC Address Group

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **MAC Sets**.

5 Select the group that you want to delete and click the **Delete** ( ) icon.

Working with IP Pools

You can edit or delete an IP pool.

For information on adding an IP pool, see "Configure Network Access SSL VPN-Plus," on page 66 or "Configure Web Access SSL VPN-Plus," on page 73.

Create an IP Pool

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **IP Pool**.

5 Click the **Add New IP Pool** icon.

6 Type a name for the IP pool and type the default gateway.

7 Type the primary and secondary DNS and the DNS suffix and the prefix length.

8 Type the IP address ranges to be included in the pool and click **OK**.

Edit an IP Pool

You can edit an IP pool.

Procedure

1 In the **SSL VPN-Plus** tab, click **IP Pool** in the left panel.

2 Select the IP pool that you want to edit.

3 Click the **Edit** ( ) icon.

The Edit IP Pool dialog box opens.

4 Make the required edits.

5 Click **OK**.

Delete IP Pool

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **IP Pool**.

5 Select the IP pool that you want to delete and click the **Delete** icon.

Working with Security Groups

A security group is a collection of assets or grouping objects from your vSphere inventory.

Create a Security Group

You create a security group at the NSX Manager level.

Prerequisites

If you are creating a security group based on Active Directory group objects, ensure that one or more domains have been registered with NSX Manager. NSX Manager gets group and user information as well as the relationship between them from each domain that it is registered with. See "Register a Windows Domain with NSX Manager," on page 164.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping** tab.

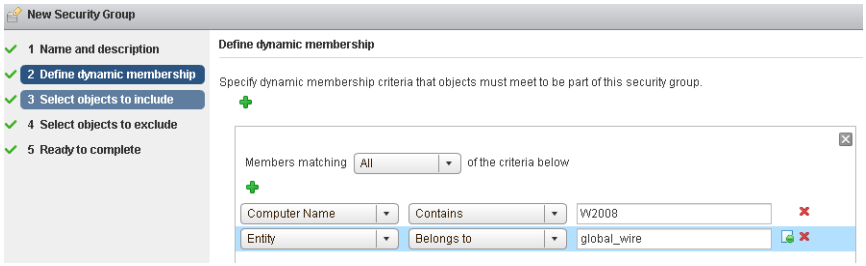
5 Click the **Security Group** tab and then click the **Add Security Group** icon.

6 Type a name and description for the security group and click **Next**.

7 On the Dynamic Membership page, define the criteria that an object must meet for it to be added to the security group you are creating. This gives you the ability to include virtual machines by defining a filter criteria with a number of parameters supported to match the search criteria.

For example, you may include a criterion to add all virtual machines tagged with the specified security tag (such as AntiVirus.virusFound) to the security group. Security tags are case sensitive.

Or you can add all virtual machines containing the name `W2008` and virtual machines that are in the logical switch `global_wire` to the security group.



8 Click **Next**.

9 On the Select objects to include page, select the tab for the resource you want to add and select one or more resources to add to the security group. You can include the following objects in a security group.

- Other security groups to nest within the security group you are creating.
- Cluster
- Logical Switch
- Network
- Virtual App
- Datacenter
- IP sets
- Directory groups

  NOTE The AD configuration for NSX security groups is different from the AD configuration for vSphere SSO. NSX AD group configuration is for end users accessing guest virtual machines, while vSphere SSO is for administrators using vSphere and NSX.

- MAC Sets
- Security tag
- vNIC
- Virtual Machine
- Resource Pool
- Distributed Virtual Port Group

The objects selected here are always included in the security group regardless of whether or not they match the criteria in Step 4.

When you add a resource to a security group, all associated resources are automatically added. For example, when you select a virtual machine, the associated vNIC is automatically added to the security group.

10 Click **Next** and select the objects that you want to exclude from the security group.

The objects selected here are always excluded from the security group regardless of whether or not they match the dynamic criteria.

11 Click **Finish**.

Membership of a security group is determined as follows:

{Expression result (derived from step 4) + Inclusions (specified in step 6} - Exclusion (specified in step 7)

This means that inclusion items are first added to the expression result. Exclusion items are then subtracted from the combined result.

Edit a Security Group

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **Security Group**.

5 Select the group that you want to edit and click the **Edit** ( ) icon.

6 In the Edit Security Group dialog box, make the appropriate changes.

7 Click **OK**.

Delete a Security Group

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **Security Group**.

5 Select the group that you want to delete and click the **Delete** ( ) icon.

Working with Services and Service Groups

A service is a protocol-port combination, and a service group is a group of services or other service groups.

Create a Service

You can create a service and then define rules for that service.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **Service**.

5 Click the **Add** icon.

6 Type a **Name** to identify the service.

7 Type a **Description** for the service.

8 Select a **Protocol** to which you want to add a non-standard port.

9 Type the port number(s) in **Ports**.

10 Click **OK**.

The service appears in the Services table.

Create a Service Group

You can create a service group and then define rules for that service group.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **Service Groups**.

5 Click **Service Groups**.

6 Click the **Add** icon.

7 Type a **Name** to identify the service group.

8 Type a **Description** for the service.

9 In Members, select the services or service groups that you want to the group.

10 Click **OK**.

Edit a Service or Service Group

You can edit services and service groups.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **Service** or **Service Groups**.

5 Select a custom service or service group and click the **Edit** ( ) icon.

6 Make the appropriate changes.

7 Click **OK**.

Delete a Service or Service Group

You can delete services or service group.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Grouping Objects** tab and then click **Service** or **Service Groups**.

5 Select a custom service or service group and click the **Delete** ( ) icon.

6 Click **Yes**.

The service or service group is deleted.

14 Operations and Management

This section describes

This chapter includes the following topics:

- "System Events and Audit Logs," on page 157
- "Management System Settings," on page 161
- "Working with Active Directory Domains," on page 164
- "NSX Edge Operations," on page 166
- "Backing Up NSX Manager Data," on page 178
- "Flow Monitoring," on page 179
- "Activity Monitoring," on page 186
- "Guest Introspection Events and Alarms," on page 195

System Events and Audit Logs

System events are events that are related to NSX operations. They are raised to detail every operational event. Events might relate to basic operation (Informational) or to a critical error (Critical).

With the NSX ticket logger feature, you can track the changes you make with a ticket ID. Audit logs for operations tracked by a ticket will include the ticket ID.

About NSX Logs

This section describes how you can configure the syslog server and view technical support logs for each NSX component. Management plane logs are available through NSX Manager and data plane logs are available through vCenter Server. Hence, it is recommended that you specify the same syslog server for the NSX component and vCenter Server in order to get a complete picture when viewing logs on the syslog server.

For information on configuring syslog for hosts managed by a vCenter Server, see VMware vSphere ESXi and vCenter Server 5.5 Documentation.

NSX Manager

To specify a syslog server, see "Specify Syslog Server," on page 161.

To download technical support logs, see "Download Technical Support Logs for NSX," on page 163.

NSX Edge

To specify a syslog server, see "Configure Remote Syslog Servers," on page 176.

To download technical support logs, see "Download Tech Support Logs for NSX Edge," on page 177.

Firewall

You must configure the remote syslog server for each cluster that has firewall enabled. The remote syslog server is specified in the `Syslog.global.logHost` attribute. See *ESXi and vCenter Server 5.5 Documentation*.

Here is a sample line from a host log file.

```
2013-10-02T05:41:12.670Z cpu11:1000046503)vsip_pkt: INET, match, PASS, Rule 0/3, Ruleset domain-c7, Rule ID 100, OUT, Len 60, SRC 10.24.106.96, DST 10.24.106.52, TCP SPORT 59692, DPORT 22 S
```

which consists of three parts:

Table 14-1. Components of log file entry

	Value in example
VMKernel common log portion consists of date, time, CPU, and WorldID	2013-10-02T05:41:12.670Z cpu11:1000046503)
Identifier	vsip_pkt
Firewall specific portion	INET, match, PASS, Rule 0/3, Ruleset domain-c7, Rule ID 100, OUT, Len 60, SRC 10.24.106.96, DST 10.24.106.52, TCP SPORT 59692, DPORT 22 S

Table 14-2. Firewall specific portion of log file entry

Entity	**Possible Values**
AF Value	INET, INET6
Reason	Possible values: match, bad-offset, fragment, short, normalize, memory, bad-timestamp, congestion, ip-option, proto-cksum, state-mismatch, state-insert, state-limit, src-limit, synproxy, spoofguard
Action	PASS, DROP, SCRUB, NOSCRUB, NAT, NONAT, BINAT, NOBINAT, RDR, NORDR, SYNPROXY_DROP, PUNT, REDIRECT, COPY
Rule identifier	*Identifier*
Rule value	Ruleset ID and Rule position (Internal details)
Rule set identifier	*Identifier*
Rule set value	Ruleset name
Rule ID identifier	*Identifier*
Rule ID	ID matched
Direction	ROUT, IN
Length identifier	Len followed by variable
Length value	Packet length
Source identifier	SRC
Source IP address	*IP address*
Destination identifier	*IP address*
Protocol	TCP, UDP, PROTO
Source port identifier	SPORT
Source port	Source port number for TDP and UDP

Table 14-2. Firewall specific portion of log file entry (Continued)

Entity	Possible Values
Source port identifier	Destination port identifier
Destination port	Destination port number for TDP and UDP
Flag	Flag for TCP

Using NSX Ticket Logger

The NSX Ticket Logger allows you to track the infrastructure changes that you make. All operations are tagged with the specified ticket ID, and audit logs for these operations include the ticket ID. Log files for these operations are tagged with the same ticked ID.

Procedure

1 Log in to the vSphere Web Client.

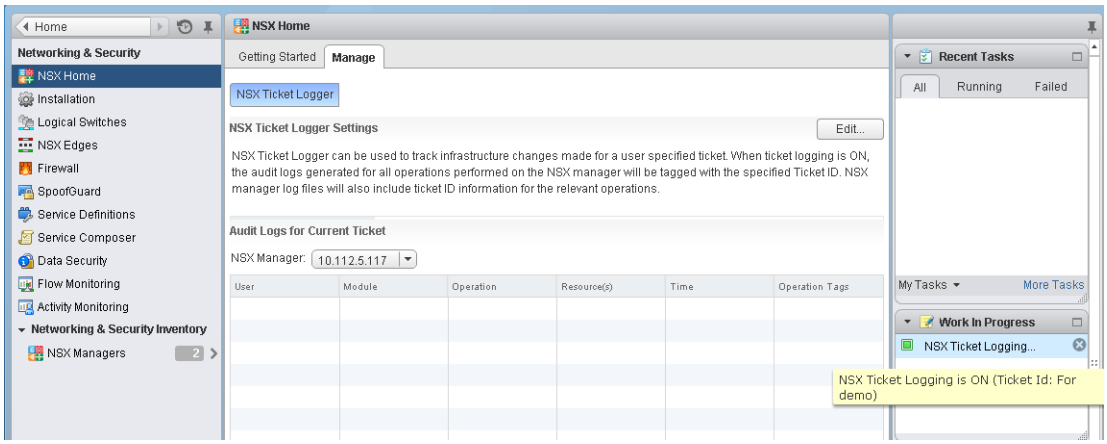
2 Click **Networking & Security** and then click the **Manage** tab.

3 Click **Edit** next to **NSX Ticket Logger Settings**.

4 Type a ticket ID and click **Turn On**.

The NSX Ticket Logging pane is displayed at the right side of the vSphere Web Client window. Audit logs for the operations that you perform in the current UI session include the ticket ID in the **Operation Tags** column.

Figure 14-1. NSX Ticket Logger pane



If multiple vCenter Servers are being managed by the vSphere Web Client, the ticket ID is used for logging on all applicable NSX Managers.

What to do next

Ticket logging is session based. If ticket logging is on and you log out or if the session is lost, ticket logging will be turned off by default when you re-login to the UI. When you complete the operations for a ticket, you turn logging off by repeating steps 2 and 3 and clicking **Turn Off**.

View the System Event Report

NSX Manager aggregates system events into a report.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Monitor** tab.

4 Click the **System Events** tab.

5 To sort events, click  or  next to the appropriate column header.

NSX Manager Virtual Appliance Events

The following events are specific to the NSX Manager virtual appliance.

Table 14-3. NSX Manager Virtual Appliance Events

	Power Off	Power On	Interface Down	Interface Up
Local CLI	Run `show log follow` command.	Run `show log follow` command.	Run `show log follow` command.	Run `show log follow` command.
GUI	NA	NA	NA	NA

Table 14-4. NSX Manager Virtual Appliance Events

	CPU	Memory	Storage
Local CLI	Run `show process monitor` command.	Run `show system memory` command.	Run `show filesystem` command.
GUI	NA	NA	NA

About the Syslog Format

The system event message logged in the syslog has the following structure.

```
syslog header (timestamp + hostname + sysmgr/)
Timestamp (from the service)
Name/value pairs
Name and value separated by delimiter '::' (double colons)
Each name/value pair separated by delimiter ';;' (double semi-colons)
```

The fields and types of the system event contain the following information.

```
Event ID :: 32 bit unsigned integer
Timestamp :: 32 bit unsigned integer
Application Name :: string
Application Submodule :: string
Application Profile :: string
Event Code :: integer (possible values: 10007 10016 10043 20019)
Severity :: string (possible values: INFORMATION LOW MEDIUM HIGH CRITICAL)
Message ::
```

View the Audit Log

The **Audit Logs** tab provides a view into the actions performed by all NSX Manager users. The NSX Manager retains up to 1,000, 000 audit logs.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click a vCNS server in the **Name** column and then click the **Monitor** tab.

4 Click the **Audit Logs** tab.

5 When details are available for an audit log, the text in the **Operation** column for that log is clickable. To view details of an audit log, click the text in the **Operation** column.

6 In the **Audit Log Change Details**, select **Changed Rows** to display only those properties whose values have changed for this audit log operation.

Management System Settings

You can edit the vCenter Server, DNS and NTP server, and Lookup server that you specified during initial login. NSX Manager requires communication with your vCenter Server and services such as DNS and NTP to provide details on your VMware Infrastructure inventory.

Log In to the NSX Manager Virtual Appliance

After you have installed and configured the NSX Manager virtual machine, log in to the NSX Manager virtual appliance to review the settings specified during installation.

Procedure

1 Open a Web browser window and type the IP address assigned to the NSX Manager. For example, **`https://11.111.11.11`**.

The NSX Manager user interface opens in a web browser window using SSL.

2 Accept the security certificate.

NOTE You can use an SSL certificate for authentication. Refer to the *NSX Administration Guide*.

The NSX Manager login screen appears.

3 Log in to the NSX Manager virtual appliance by using the user name **`admin`** and the password you set during installation. If you had not set a password during installation, type **`default`** as the password.

4 Click **Log In**.

Edit the NSX Manager Date and Time

You can change the NTP server specified during initial login.

Procedure

1 Log in to the NSX Manager virtual appliance.

2 Under **Appliance Management**, click **Manage Appliance Settings**.

3 Click **Edit** next to **Time Settings**.

4 Make the appropriate changes.

5 Click **OK**.

6 Reboot the NSX Manager.

Specify Syslog Server

If you specify a syslog server, NSX Manager sends all audit logs and system events from NSX Manager to the syslog server.

Procedure

1 Log in to the NSX Manager virtual appliance.

2 Under **Appliance Management**, click **Manage Appliance Settings**.

3 From the Settings panel, click **General**.

4 Click **Edit** next to **Syslog Server**.

5 Type the IP address of the syslog server.

6 Type the port and protocol for the syslog server.

If you do not specify a port, the default UDP port for the IP address/host name of the syslog server is used.

7 Click **OK**.

Edit DNS Servers

You can change the DNS servers specified during Manager installation.

Procedure

1 Log in to the NSX Manager virtual appliance.

2 Under **Appliance Management**, click **Manage Appliance Settings**.

3 From the Settings panel, click **Network**.

4 Click **Edit** next to **DNS Servers**.

5 Make the appropriate changes.

6 Click **OK**.

Edit Lookup Service Details

You can change the Lookup Service details specified during initial login.

Procedure

1 Log in to the NSX Manager virtual appliance.

2 Under **Appliance Management**, click **Manage Appliance Settings**.

3 From the Settings panel, click **NSX Management Service**.

4 Click **Edit** next to **Lookup Service**.

5 Make the appropriate changes.

6 Click **OK**.

Edit vCenter Server

You can change the vCenter Server with which you registered NSX Manager during installation. You should do this only if you change the IP address of your current vCenter Server.

Procedure

1 If you are logged in to the vSphere Web Client, log out.

2 Log in to the NSX Manager virtual appliance.

3 Under **Appliance Management**, click **Manage Appliance Settings**.

4 From the Settings panel, click **NSX Management Service**.

5 Click **Edit** next to **vCenter Server**.

6 Make the appropriate changes.

7 Click **OK**.

Download Technical Support Logs for NSX

You can download NSX Manager system logs and Web Manager logs to your desktop.

Procedure

1 Log in to the NSX Manager virtual appliance.

2 Under Appliance Management, click **Manage Appliance Settings**.

3 Click  and then click **Download Tech Support Log**.

4 Click **Download**.

5 After the log is ready, click the **Save** to download the log to your desktop.

The log is compressed and has the file extension `.gz`.

What to do next

You can open the log using a decompression utility by browsing for **All Files** in the directory where you saved the file.

Add an SSL Certificate to Identify the NSX Manager Web Service

You can generate a certificate signing request, get it signed by a CA, and import the signed SSL certificate into NSX Manager to authenticate the identity of the NSX Manager web service and encrypt information sent to the NSX Manager web server. As a security best practice, you should use the generate certificate option to generate a private key and public key, where the private key is saved to the NSX Manager.

Procedure

1 Log in to the NSX Manager virtual appliance.

2 Under **Appliance Management**, click **Manage Settings**.

3 From the Settings panel, click **SSL Certificate**.

4 Under **Generate Certificate Signing Request**, complete the form by filling in the following fields:

Option	Action
Key Size	Select the key length used in the selected algorithm.
Common Name	Type the IP address or fully qualified domain name (FQDN) of the NSX Manager. VMware recommends that you enter the FQDN.
Organization Unit	Enter the department in your company that is ordering the certificate.
Organization Name	Enter the full legal name of your company.
City Name	Enter the full name of the city in which your company resides.
State Name	Enter the full name of the state in which your company resides.
Country Code	Enter the two-digit code that represents your country. For example, the United States is **US**.

5 Click **OK**.

Import an SSL certificate

You can import a pre-existing or CA signed SSL certificate for use by the NSX Manager.

Procedure

1 Log in to the NSX Manager virtual appliance.

2 Under **Appliance Management**, click **Manage Settings**.

3 From the Settings panel, click **SSL Certificates** and then click **Import**.

4 Click **Browse** to locate the file.

5 Click **Import**.

A yellow bar containing the message **Successfully imported certificate** is displayed at the top of the screen.

6 Click **Apply Certificate**.

NSX Manager is restarted to apply the certificate.

The certificate is stored in NSX Manager.

Working with Active Directory Domains

You can a register one or more Windows domains with an NSX Manager and associated vCenter server. NSX Manager gets group and user information as well as the relationship between them from each domain that it is registered with. NSX Manager also retrieves Active Directory (AD) credentials.

Once NSX Manager retrieves AD credentials, you can create security groups based on user identity, create identity-based firewall rules, and run Activity Monitoring reports.

Register a Windows Domain with NSX Manager

Prerequisites

The domain account must have AD read permission for all objects in the domain tree. The event log reader account must have read permissions for security event logs.

Procedure

1 Log in to the vSphere Web Client. 2. 3.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Click the **Domain** tab and then click the **Add domain** ( ) icon.

5 In the Add Domain dialog box, enter the fully qualified domain name (for example, `eng.vmware.com`) and netBIOS name for the domain.

To retrieve the netBIOS name for your domain, type `nbstat –n` in a command window on a Windows workstation that is part of a domain or on a domain controller. In the NetBIOS Local Name Table, the entry with a <00> prefix and type Group is the netBIOS name.

6 Click **Next**.

7 In the LDAP Options page, specify the domain controller that the domain is to be synchronized with and select the protocol.

8 Edit the port number if required.

9 Enter the user credentials for the domain account. This user must be able to access the directory tree structure.

10 Click **Next**.

11 In the Security Event Log Access page, select the connection method to access security event logs on the specified LDAP server. Change the port number if required.

12 Select **Use Domain Credentials** to use the LDAP server user credentials. To specify an alternate domain account for log access, un-select **Use Domain Credentials** and specify the user name and password.

The specified account must be able to read the security event logs on the Domain Controller specified in step 10.

13 Click **Next**.

14 In the Ready to Complete page, review the settings you entered.

15 Click **Finish**.

The domain is created and its settings are displayed below the domain list.

What to do next

Verify that login events on the event log server are enabled.

You can add, edit, delete, enable, or disable LDAP servers by selecting the **LDAP Servers** tab in the panel below the domain list. You can perform the same tasks for event log servers by selecting the **Event Log Servers** tab in the panel below the domain list. Adding more than one Windows server (Domain Controllers, Exchange servers, or File Servers) as an event log server improves the user identity association.

Synchronize a Windows Domain with Active Directory

By default, all registered domains are automatically synchronized with Active Directory every 3 hours. You can also synchronize on demand.

Procedure

1 Log in to the vSphere Web Client. 2. 3.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Select the domain to be synchronized.

5 Click one of the following.

Click	To
	Perform a delta synchronization, where local AD objects that changed since the last synchronization event are updated
	Perform a full synchronization, where the local state of all AD objects is updated

Edit a Windows Domain

You can edit the name, netBIOS name, primary LDAP server, and account credentials of a domain.

Procedure

1 Log in to the vSphere Web Client. 2. 3.

2 Click **Networking & Security** and then click **NSX Managers**.

3 Click an NSX Manager in the **Name** column and then click the **Manage** tab.

4 Select a domain and then click the **Edit domain** icon.

5 Make the desired changes and click **Finish**.

NSX Edge Operations

If you installed a working NSX Edge (i.e. added one or more appliances and interfaces, and configured the default gateway, firewall policy, and high availability), you can begin using NSX Edge services.

If you did not do one or more of the above tasks and the NSX Edge is not deployed, you may need to follow some of the instructions in this topic before you can use NSX Edge services.

Working with Certificates

NSX Edge supports self-signed certificates, certificates signed by a Certification Authority (CA), and certificates generated and signed by a CA.

Configure a CA Signed Certificate

You can generate a CSR and get it signed by a CA. If you generate a CSR at the global level, it is available to all NSX Edges in your inventory.

Procedure

1 Do one of the following.

Option	Description
To generate a global certificate	a Log in to the NSX Manager Virtual Appliance. b Click the Manage tab and then click SSL Certificates. c Click **Generate CSR**.
To generate a certificate for an NSX Edge	a Log in to the vSphere Web Client. b Click **Networking & Security** and then click **Edge Services**. c Double-click an NSX Edge. d Click the **Manage** tab and then click **Settings**. e Click the **Certificates** link. f Click **Actions** and select **Generate CSR**.

2 Type your organization unit and name.

3 Type the locality, street, state, and country of your organization.

4 Select the encryption algorithm for communication between the hosts.

Note that SSL VPN-Plus only supports RSA certificates.

5 Edit the default key size if required.

6 For a global certificate, type a description for the certificate.

7 Click **OK**.

The CSR is generated and displayed in the Certificates list.

8 Have an online Certification Authority sign this CSR.

9 Import the signed certificate.

a Copy the contents of the signed certificate.

b Do one of the following.

- To import a signed certificate at the global level, click **Import** in the NSX Manager Virtual Appliance.
- To import a signed certificate for an NSX Edge, click **Actions** and select **Import Certificate** in the **Certificates** tab.

c In the Import CSR dialog box, paste the contents of the signed certificate.

d Click **OK**.

The CA signed certificate appears in the certificates list.

Add a CA Certificate

By adding a CA certificate, you can become an interim CA for your company. You then have the authority for signing your own certificates.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then ensure that you are in the **Settings** tab.

5 Click **Certificates**.

6 Click the **Add** ( ) icon and select **CA Certificate.**

7 Copy and paste the certificate contents in the Certificate contents text box.

8 Type a description for the CA certificate.

9 Click **OK**.

You can now sign your own certificates.

Configure a Self-Signed Certificate

You can create, install, and manage self-signed server certificates.

Prerequisites

Verify that you have a CA certificate so that you can sign your own certificates.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then ensure that you are in the **Settings** tab.

5 Click **Certificates**.

6 Follow the steps below to generate a CSR.

   a Click **Actions** and select **Generate CSR**.

   b In Common name, type the IP address or fully qualified domain name (FQDN) of the NSX Manager.

   c Type your organization name and unit.

   d Type the locality, street, state, and country of your organization.

   e Select the encryption algorithm for communication between the hosts.

      Note that SSL VPN-Plus only supports RSA certificates. VMware recommends RSA for backward compatibility.

   f Edit the default key size if required.

   g Type a description for the certificate.

   h Click **OK**.

   The CSR is generated and displayed in the Certificates list.

7 Verify that the certificate you generated is selected.

8 Click **Actions** and select **Self Sign Certificate**.

9 Type the number of days the self sign certificate is valid for.

10 Click **OK**.

Using Client Certificates

You can create a client certificate through a CAI command or REST call. You can then distribute this certificate to your remote users, who can install the certificate on their web browser

The main benefit of implementing client certificates is that a reference client certificate for each remote user can be stored and checked against the client certificate presented by the remote user. To prevent future connections from a certain user, you can delete the reference certificate from the security server's list of client certificates. Deleting the certificate denies connections from that user.

Add a Certificate Revocation List

A Certificate Revocation List (CRL) is a list of subscribers and their status, which is provided and signed by Microsoft.

The list contains the following items:

- The revoked certificates and the reasons for revocation
- The dates that the certificates are issued
- The entities that issued the certificates
- A proposed date for the next release

When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then ensure that you are in the **Settings** tab.

5 Click **Certificates**.

6 Click the **Add** ( ) icon and select **CRL**.

7 In **Certificate contents**, paste the list.

8 (Optional) Type a description.

9 Click **OK**.

Managing Appliances

You can add, edit, or delete appliances. An NSX Edge instance remains offline till at least one appliance has been added to it.

Add an Appliance

You must add at least one appliance to NSX Edge before deploying it.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **Settings** tab.

5 In **Edge Gateway Appliances**, click the **Add** ( ) icon.

6 Select the cluster or resource pool and datastore for the appliance.

7 (Optional) Select the host on which the appliance is to be added.

8 (Optional) Select the vCenter folder within which the appliance is to be added.

9 Click **Add**.

Edit an Appliance

You can edit a NSX Edge appliance.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **Settings** tab.

5 In **Edge Gateway Appliances**, select the appliance to change.

6 Click the **Edit** ( ) icon.

7 In the Edit Edge Appliance dialog box, make the appropriate changes.

8 Click **Save**.

Delete an Appliance

You can delete an NSX Edge appliance.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **Settings** tab.

5 In **Edge Gateway Appliances**, select the appliance to delete.

6 Click the **Delete** ( ) icon.

Working with Interfaces

An NSX Edge services gateway can have up to ten internal, uplink, or trunk interfaces. An NSX Edge router can have eight uplink interfaces and up to a thousand internal interfaces.

An NSX Edge must have at least one internal interface before it can be deployed.

Configure an Interface

An NSX Edge services gateway can have up to ten internal, uplink, or trunk interfaces. An NSX Edge router can have eight uplink interfaces and up to a thousand internal interfaces.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **Interfaces** tab.

5 Select an interface and click the **Edit** ( ) icon.

6 In the Edit Edge Interface dialog box, type a name for the interface.

7 Select **Internal** or **Uplink** to indicate whether this is an internal or external interface.

Select **Trunk** when creating a sub interface. For more information, see "Add a Sub Interface," on page 172.

8 Select the port group or logical switch to which this interface should be connected.

a Click **Select** next to the **Connected To** field.

b Depending on what you want to connect to the interface, click the **Logical Switch**, **Standard Portgroup**, or **Distributed Portgroup** tab.

c Select the appropriate logical switch or portgroup.

d Click **Select**.

9 Select the connectivity status for the interface.

10 In **Configure Subnets**, click the **Add** ( ) icon to add a subnet for the interface.

An interface can have multiple non-overlapping subnets.

11 In **Add Subnet**, click the **Add** ( ) icon to add an IP address.

If you enter more than one IP address, you can select the Primary IP address. An interface can have one primary and multiple secondary IP addresses. NSX Edge considers the Primary IP address as the source address for locally generated traffic.

You must add an IP address to an interface before using it on any feature configuration.

12 Type the subnet mask for the interface and click **Save**.

13 Change the default MTU if required.

14 In **Options**, select the required options.

Option	Description
Enable Proxy ARP	Supports overlapping network forwarding between different interfaces.
Send ICMP Redirect	Conveys routing information to hosts.

15 Type the fence parameters and click **Add**.

16 Click **OK**.

Delete an Interface

You can delete an NSX Edge interface.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **Interfaces** tab.

5 Select the interface to delete.

6 Click the **Delete** ( ) icon

Enable an Interface

An interface must be enabled for NSX Edge to isolate the virtual machines within that interface (port group or logical switch).

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **Interfaces** tab.

5 Select the interface to enable.

6 Click the **Enable** ( ) icon.

Disable an Interface

You can disable an interface

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **Interfaces** tab.

5 Select the interface to disable.

6 Click the **Disable** icon.

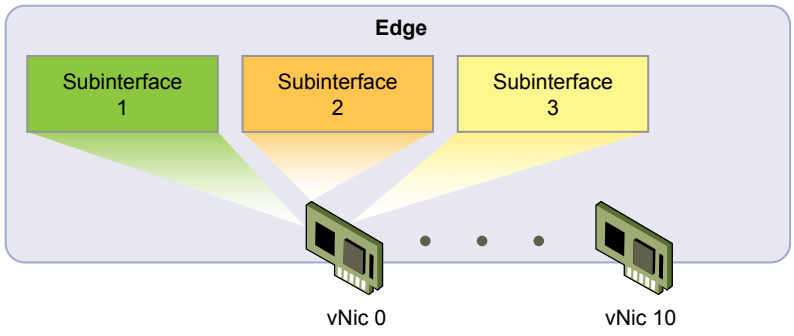
Change Traffic Shaping Policy

You can change the traffic shaping policy on the vSphere Distributed Switch for the NSX Edge.

For more information, see Traffic Shaping Policy.

Add a Sub Interface

You can add a sub interface on a trunk vNIC, which can then be used by NSX Edge services.



Trunk interfaces can be of the following types:

- VLAN trunk is standard and work with any version of ESXi. This is used to bring tagged VLAN traffic into Edge.
- VXLAN trunk work only with NSX version 6.1. This is used to bring VXLAN traffic into Edge.

A sub interface can be used by the following Edge services:

- DHCP
- NAT (DNAT only)
- Routing (BGP only)
- Load Balancer
- IPSEC VPN
- L2 VPN

A sub interface cannot be used for HA or Logical Firewall. You can, however, use the IP address of the sub interface in a firewall rule.

Procedure

1 In the **Manage > Settings** tab for an NSX Edge, click **Interfaces**.

2 Select an interface and click the **Edit** ( ) icon.

3 In the Edit Edge Interface dialog box, type a name for the interface.

4 In Type, select **Trunk**.

5 Select the standard portgroup or distributed portgroup to which this interface should be connected.

   a Click **Change** next to the **Connected To** field.

   b Depending on what you want to connect to the interface, click the **Standard Portgroup** or **Distributed Portgroup** tab.

   c Select the appropriate portgroup and click **OK**.

   d Click **Select**.

6 In Sub Interfaces, click the **Add** icon.

7 Click **Enable Sub interface** and type a name for the sub interface.

8 In **Tunnel Id**, type a number between 1 and 4094.

   The tunnel Id is used to connect the networks that are being stretched. This value must be the same on both the client and server sites.

9 In Backing Type, select one of the following to indicate the network backing for the sub interface.

   - **VLAN** for a VLAN network.

     Type the VLAN ID of the virtual LAN that your sub interface should use. VLAN IDs can range from 0 to 4094.

   - **Network** for a VLAN or VXLAN network.

     Click **Select** and select the distributed portgroup or logical switch. NSX Manager extracts the VLAN ID and uses it in trunk configuration.

   - **None** to create a sub interface without specifying a network or VLAN ID. This sub interface is internal to NSX Edge, and is used to route packets between a stretched network and an unstretched (untagged) network

10 To add subnets to the sub interface, click the **Add** icon in the Configure Subnets area.

11 In Add Subnets, click the **Add** icon to add an IP address. Type the IP address and click **OK**.

   If you enter more than one IP address, you can select the Primary IP address. An interface can have one primary and multiple secondary IP addresses. NSX Edge considers the Primary IP address as the source address for locally generated traffic.

12 Type the subnet prefix length and click **OK**.

13 Edit the default **MTU** value for the sub interface if required.

   The default MTU for a trunk interface is 1600 and the default MTU for a sub interface is 1500. The MTU for the sub interface should be equal to or less than the lowest MTU among all the trunk interfaces for the NSX Edge.

14 Select **Enable Send Redirect** to convey routing information to hosts.

15 Type the MAC address for the interface.

   Since sub interfaces do not support HA, only one MAC address is required.

16 Edit the default MTU of the trunk interface, if required.

17 Click **OK**.

You can now use the sub-interface on Edge services.

What to do next

When the sub interface is added to a trunk vNic backed by distributed portgroup, VLAN or VXLAN trunk is automatically configured on the trunk port. When the sub interface is added to a trunk vNic backed by standard portgroup, only VLAN trunk is supported. VLAN trunk must be manually configured by following the steps below:

1 Log in to the vCenter Web Client.

2 Click **Networking**.

3 Select the standard portgroup and click **Edit Settings**.

4 Click the VLAN tab.

5 In VLAN Type, select VLAN Trunking and type the VLAN IDs to be trunked.

6 Click **OK**.

Change Auto Rule Configuration

If auto rule generation is enabled, NSX Edge adds firewall, NAT, and routing routes to enable control traffic to flow for these services. If auto rule generation is not enabled, you must manually add firewall, NAT, and routing configuration to allow control channel traffic for NSX Edge services such as Load Balancing, VPN, etc.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click the **Settings** tab.

5 Click the **More Actions** ( ) icon and select **Change Auto Rule configuration**.

6 Make the appropriate changes and click **OK**.

Change CLI Credentials

You can edit the credentials to be used for logging in to the Command Line Interface (CLI).

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click the **Settings** tab.

5 Click the **More Actions** ( ) icon and select **Change CLI Credentials**.

6 Make the appropriate edits.

7 Click **OK**.

About High Availability

High Availability (HA) ensures that an NSX Edge appliance is always available by installing an active pair of Edges on your virtualized infrastructure. You can enable HA either when installing NSX Edge or on an installed NSX Edge instance.

Stateful High Availability

The primary NSX Edge appliance is in the active state and the secondary appliance is in the standby state. NSX Edge replicates the configuration of the primary appliance for the standby appliance or you can manually add two appliances. VMware recommends that you create the primary and secondary appliances on separate resource pools and datastores. If you create the primary and secondary appliances on the same datastore, the datastore must be shared across all hosts in the cluster for the HA appliance pair to be deployed on different ESX hosts. If the datastore is a local storage, both virtual machines are deployed on the same host.

All NSX Edge services run on the active appliance. The primary appliance maintains a heartbeat with the standby appliance and sends service updates through an internal interface.

If a heartbeat is not received from the primary appliance within the specified time (default value is 15 seconds), the primary appliance is declared dead. The standby appliance moves to the active state, takes over the interface configuration of the primary appliance, and starts the NSX Edge services that were running on the primary appliance. When the switch over takes place, a system event is displayed in the **System Events** tab of Settings & Reports. Load Balancer and VPN services need to re-establish TCP connection with NSX Edge, so service is disrupted for a short while. Logical switch connections and firewall sessions are synched between the primary and standby appliances, so there is no service disruption during switch over.

If the NSX Edge appliance fails and a bad state is reported, HA force syncs the failed appliance in order to revive it. When revived, it takes on the configuration of the now-active appliance and stays in a standby state. If the NSX Edge appliance is dead, you must delete the appliance and add a new one.

NSX Edge ensures that the two HA NSX Edge virtual machines are not on the same ESX host even after you use DRS and vMotion (unless you manually vMotion them to the same host). Two virtual machines are deployed on vCenter in the same resource pool and datastore as the appliance you configured. Local link IPs are assigned to HA virtual machines in the NSX Edge HA so that they can communicate with each other. You can specify management IP addresses to override the local links.

If syslog servers are configured, logs on the active appliance are sent to the syslog servers.

vSphere High Availability

NSX Edge HA is compatible with vSphere HA. If the host on which a NSX Edge instance is running dies, the NSX Edge is restarted on the standby host thereby ensuring the NSX Edge HA pair is still available to take another failover.

If vSphere HA is not leveraged, the active-standby NSX Edge HA pair will survive one fail-over. However, if another fail-over happens before the second HA pair was restored, NSX Edge availability can be compromised.

For more information on vSphere HA, see *vSphere Availability*.

Change HA Configuration

You can change the HA configuration that you had specified while installing NSX Edge.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Manage** tab and then click the **Settings** tab.

5 In the **HA Configuration** panel, click **Change**.

6 In the Change HA Configuration dialog box, make changes as appropriate.

7 Click **OK**.

Synchronize NSX Edge with NSX Manager

You can send a synchronization request from NSX Manager to NSX Edge.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Select an NSX Edge instance.

4 Click the **More Actions** ( ) icon and select **Force Sync**.

Configure Remote Syslog Servers

You can configure one or two remote syslog servers. NSX Edge events and logs related to firewall events that flow from NSX Edge appliances are sent to the syslog servers.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click a NSX Edge.

4 Click the **Monitor** tab and then click the **Settings** tab.

5 In the **Details** panel, click **Change** next to Syslog servers.

6 Type the IP address of both remote syslog servers and select the protocol.

7 Click **OK** to save the configuration.

View the Status of an NSX Edge

The status page displays graphs for the traffic flowing through the interfaces of the selected NSX Edge and connection statistics for the firewall and load balancer services.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab.

5 Select the period for which you want to view the statistics.

What to do next

To view more details about NSX Edge, click **Manage** and then click **Settings**.

Redeploy NSX Edge

If NSX Edge services do not work as expected after a force sync, you can redeploy the NSX Edge instance.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Select an NSX Edge instance.

4 Click the **More Actions** () icon and select **Redeploy Edge**.

The NSX Edge virtual machine is replaced with a new virtual machine and all services are restored. If redeploy does not work, power off the NSX Edge virtual machine and redeploy NSX Edge again.

NOTE Redeploy may not work in the following cases.

- Resource pool on which the NSX Edge was installed is no longer in the vCenter inventory or its Managed Object ID (MoId) has changed.
- Datastore on which the NSX Edge was installed is corrupted/unmounted or in-accessible.
- dvportGroups on which the NSX Edge interfaces were connected are no longer in the vCenter inventory or their MoId (identifier in vCenter server) has changed.

If any of the above is true, you must update the MoId of the resource pool, datastore, or dvPortGroup using a REST API call. See *NSX API Programming Guide*.

Download Tech Support Logs for NSX Edge

You can download technical support logs for each NSX Edge instance. If high availability is enabled for the NSX Edge instance, support logs from both NSX Edge virtual machines are downloaded.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Select an NSX Edge instance.

4 Click the **More Actions** () icon and select **Download Tech Support Logs**.

5 After the tech support logs are generated, click **Download**.

6 In the Select location for download dialog box, browse to the directory where you want to save the log file.

7 Click **Save**.

8 Click **Close**.

Upgrade NSX Edge

You can upgrade an NSX Edge instance.

Prerequisites

- A Compact NSX Edge instance requires 256 MB memory and 300 MB disk space.
- A Large NSX Edge instance requires 1024 MB memory and 448 MB disk space.

- A Quad Large NSX Edge instance requires 1024 MB memory and 448 MB disk space. This provides additional throughput over other form factors.
- An X-Large NSX Edge instance requires 8 GB memory and 448 MB disk space. An x-large NSX Edge instance is recommended for an environment where the Load Balancer service is being used on millions of concurrent sessions.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Select a compact NSX Edge instance.

4 Click the **More Actions** () icon and select **Convert to Large**, **Convert to X-Large**, or **Convert to Quad Large**.

The NSX Edge instance is upgraded.

Backing Up NSX Manager Data

You can back up and restore your NSX Manager data, which can include system configuration, events, and audit log tables. Configuration tables are included in every backup. Backups are saved to a remote location that must be accessible by the NSX Manager.

Back Up Your NSX Manager Data

You can back up NSX Manager data at any time by performing an on-demand backup.

Procedure

1 Log in to the NSX Manager Virtual Appliance.

2 Under Appliance Management, click **Backups & Restore**.

3 To specify the backup location, click **Change** next to FTP Server Settings.

a Type the IP address or host name of the backup system.

b From the **Transfer Protocol** drop-down menu, select either **SFTP** or **FTP**, based on what the destination supports.

c Edit the default port if required.

d Type the user name and password required to login to the backup system.

e In the **Backup Directory** field, type the absolute path where backups will be stored.

f Type a text string in **Filename Prefix**.

This text is prepended to each backup filename for easy recognition on the backup system. For example, if you type **ppdb**, the resulting backup is named as `ppdbHH_MM_SS_DayDDMonYYYY`.

g Type the pass phrase to secure the backup.

h Click **OK**.

4 To specify schedule details, click **Change** next to Scheduling.

   a From the **Backup Frequency** drop-down menu, select **Hourly**, **Daily**, or **Weekly**. The Day of Week, Hour of Day, and Minute drop-down menus are disabled based on the selected frequency. For example, if you select Daily, the Day of Week drop-down menu is disabled as this field is not applicable to a daily frequency.

   b For a weekly backup, select the day of the week the data should be backed up.

   c For a weekly or daily backup, select the hour at which the backup should begin.

   d Select the minute at which the begin and click **Schedule**.

5 To exclude logs and flow data from being backed up, click **Change** next to Exclude.

   a Select the items you want to exclude from the backup.

   b Click **OK**.

Restore a Backup

You can restore a backup only on a freshly deployed NSX Manager appliance.

To restore an available backup, the **Host IP Address**, **User Name**, **Password**, and **Backup Directory** fields in the **Backups** screen must have values that identify the location of the backup to be restored.

IMPORTANT Back up your current data before restoring a backup file.

Procedure

1 Log in to the NSX Manager Virtual Appliance.

2 Under Appliance Management, click **Backups & Restore**.

3 In the Backups History section, select the check box for the backup to restore.

4 Click **Restore**.

5 Click **OK** to confirm.

Flow Monitoring

Flow Monitoring is a traffic analysis tool that provides a detailed view of the traffic to and from protected virtual machines. When flow monitoring is enabled, its output defines which machines are exchanging data and over which application. This data includes the number of sessions and packets transmitted per session. Session details include sources, destinations, applications, and ports being used. Session details can be used to create firewall allow or block rules.

You can view TCP and UDP connections to and from a selected vNIC. You can also exclude flows by specifying filters.

Flow Monitoring can thus be used as a forensic tool to detect rogue services and examine outbound sessions.

Configure Flow Monitoring

Flow collection must be enabled for you to view traffic information. You can filter the data being displayed by specifying exclusion criterion.

For example, you may want to exclude a proxy server to avoid seeing duplicate flows. Or if you are running a Nessus scan on the virtual machines in your inventory, you may not want to exclude the scan flows from being collected.

You can configure IPFix so that information for specific flows are exported directly from Firewall to a flow collector. The flow monitoring graphs do not include the IPFix flows - these are displayed on the IPFix collector's interface.

Procedure

1 Log in to the vSphere Web Client.

2 Select **Networking & Security** from the left navigation pane and then select **Flow Monitoring**.

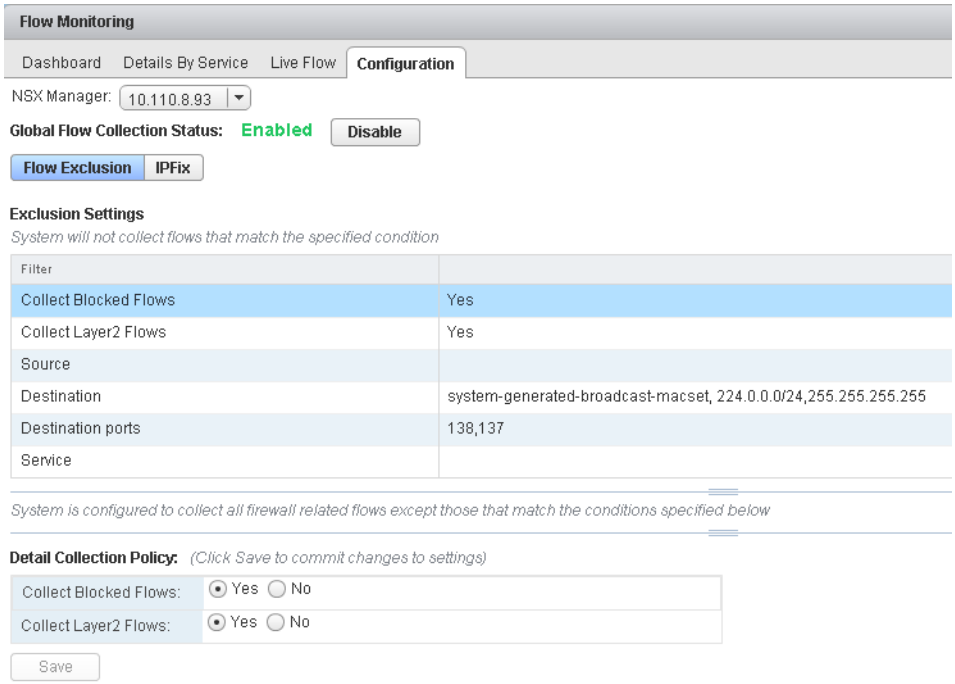
3 Select the **Configuration** tab.

4 Ensure that **Global Flow Collection Status** is **Enabled**.

All firewall related flows are collected across your inventory except for the objects specified in **Exclusion Settings**.

5 To specify filtering criterion, click **Flow Exclusion** and follow the steps below.

a Click the tab corresponding to the flows you want to exclude.



b Specify the required information.

If you selected	Specify the following information
Collect Blocked Flows	Select No to exclude blocked flows.
Collect Layer2 Flows	Select No to exclude Layer2 flows.
Source	Flows are not collected for the specified sources. 1 Click the **Add** icon. 2 In View, select the appropriate container. 3 Select the objects to exclude.
Destination	Flows are not collected for the specified destinations. 1 Click the **Add** icon. 2 In View, select the appropriate container. 3 Select the objects to exclude.
Destination ports	Excludes flows to the specified ports. Type the port numbers to exclude.
Service	Excludes flows for the specified services and service groups. 1 Click the **Add** icon. 2 Select the appropriate services and/or service groups.

c Click **Save**.

6 To configure flow collection, click **IPFix** and follow the steps below.

a Click **Edit** next to IPFix Configuration and click **Enable IPFix Configuration**.

b In **Observation DomainID**, type a 32-bit identifier that identifies the firewall exporter to the flow collector.

c In **Active Flow Export Timeout**, type the time (in minutes) after which active flows are to be reported to the flow collector. The default value is 5. For example, if the flow is active for 30 minutes and the export timeout is 5 minutes, then the flow will be exported 7 times during it's lifetime. Once each for creation and deletion, and 5 times during the active period.

d In **Collector IPs**, click the Add ( ) icon and type the IP address and UDP port of the flow collector.

e Click **OK**.

View Flow Monitoring Data

You can view traffic sessions on virtual machines within the specified time span. The last 24 hours of data are displayed by default, the minimum time span is one hour and the maximum is two weeks.

Prerequisites

Flow monitoring data is only available for virtual machines in clusters that have the network virtualization components installed and firewall enabled. See the *NSX Installation and Upgrade Guide*.

Procedure

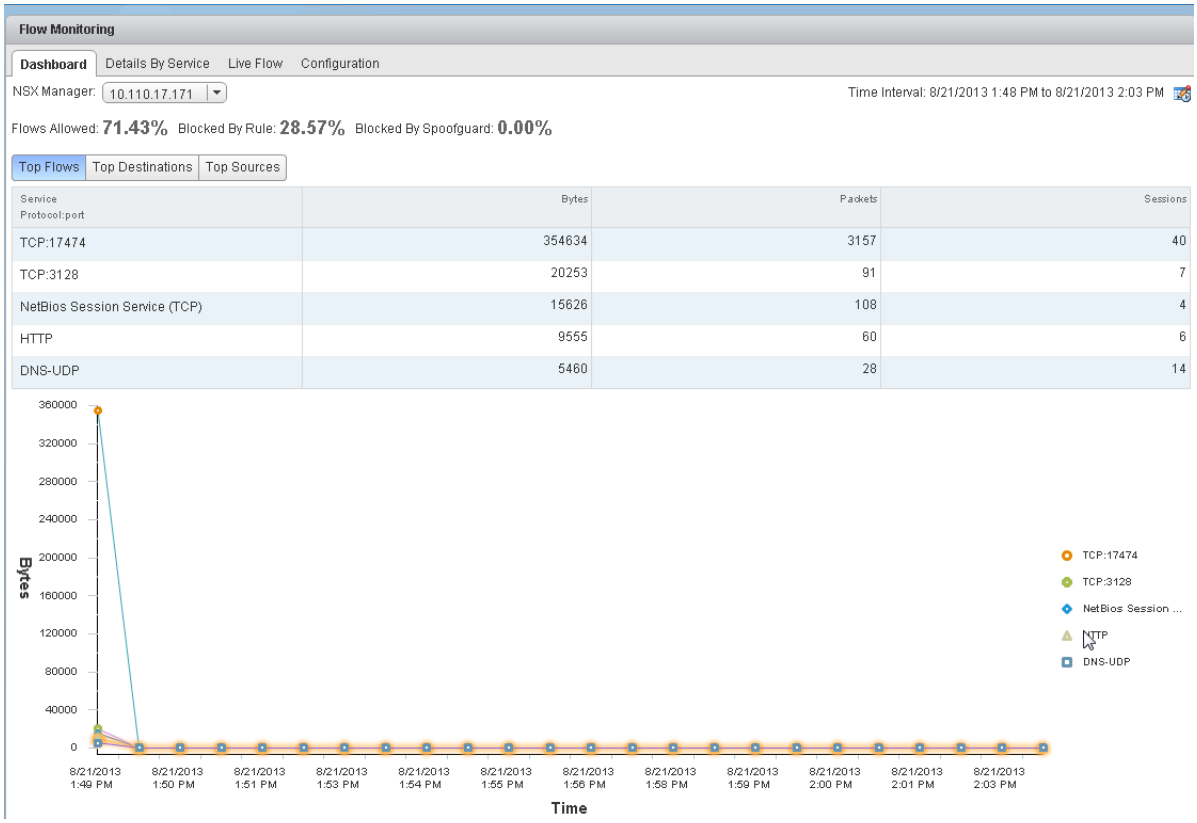
1 Log in to the vSphere Web Client.

2 Select **Networking & Security** from the left navigation pane and then select **Flow Monitoring**.

3 Ensure that you are in the **Dashboard** tab.

4 Click **Flow Monitoring**.

The page might take several seconds to load. The top of the page displays the percentage of allowed traffic, traffic blocked by firewall rules, and traffic blocked by SpoofGuard. The multiple line graph displays data flow for each service in your environment. When you point to a service in the legend area, the plot for that service is highlighted.



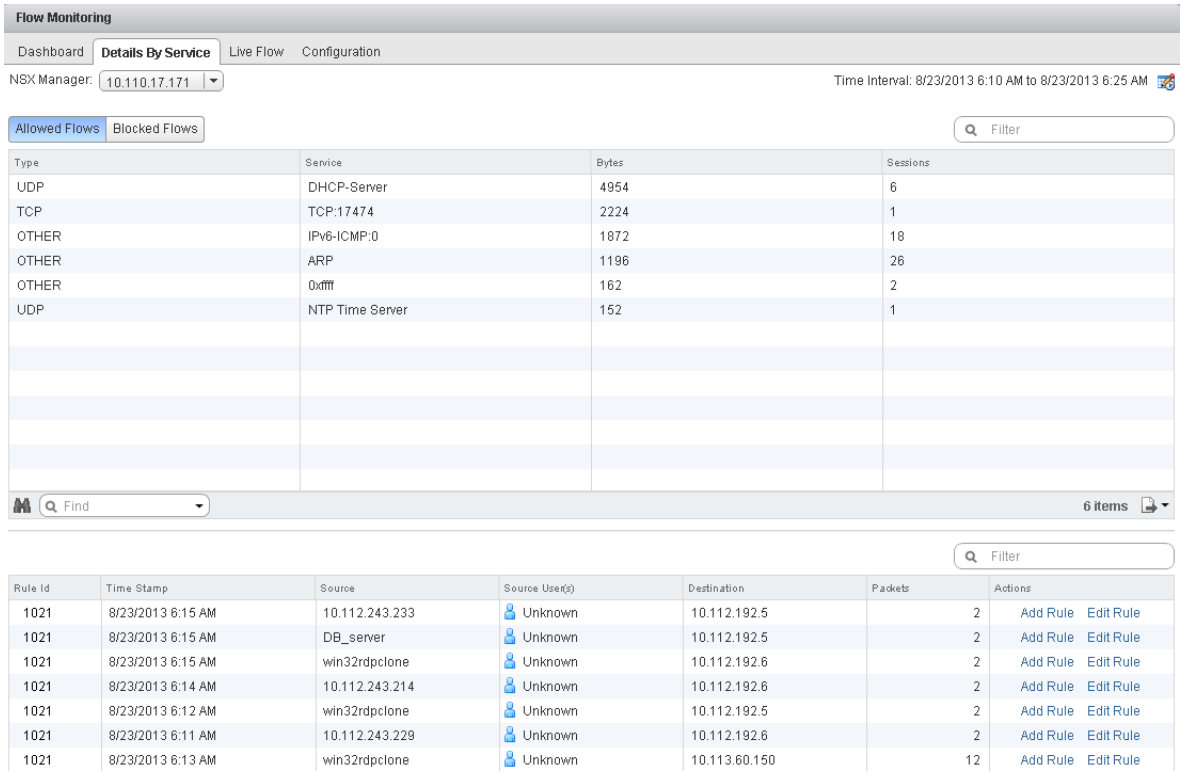
Traffic statistics are displayed in three tabs:

- **Top Flows** displays the total incoming and outgoing traffic per service over the specified time period based on the total bytes value (not based on sessions/packets). The top five services are displayed. Blocked flows are not considered when calculating top flows.
- **Top Destinations** displays incoming traffic per destination over the specified time period. The top five destinations are displayed.
- **Top Sources** displays outgoing traffic per source over the specified time period. The top five sources are displayed.

5 Click the **Details by Service** tab.

Details about all traffic for the selected service is displayed. Click **Load More Records** to display additional flows. The **Allowed Flows** tab displays the allowed traffic sessions and the **Blocked Flows** tab displays the blocked traffic.

You can search on service names.



6 Click an item in the table to display the rules that allowed or blocked that traffic flow.

7 Click the **Rule Id** for a rule to display the rule details.

Change the Date Range of the Flow Monitoring Charts

You can change the date range of the flow monitoring data for both the Dashboard and Details tabs.

Procedure

1 Log in to the vSphere Web Client.

2 Select **Networking & Security** from the left navigation pane and then select **Flow Monitoring**.

3 Click  next to **Time interval**.

4 Select the time period or type a new start and end date.

The maximum time span for which you can view traffic flow data is the previous two weeks.

5 Click **OK**.

View Live Flow

You can view UDP and TCP connections from and to a selected vNIC. In order to view traffic between two virtual machines, you can view live traffic for one virtual machine on one computer and the other virtual machine on a second computer. You can view traffic for a maximum of two vNICs per host and for 5 vNICs per infrastructure.

Viewing live flows can affect the performance of NSX Manager and the corresponding virtual machine.

Procedure

1 Log in to the vSphere Web Client.

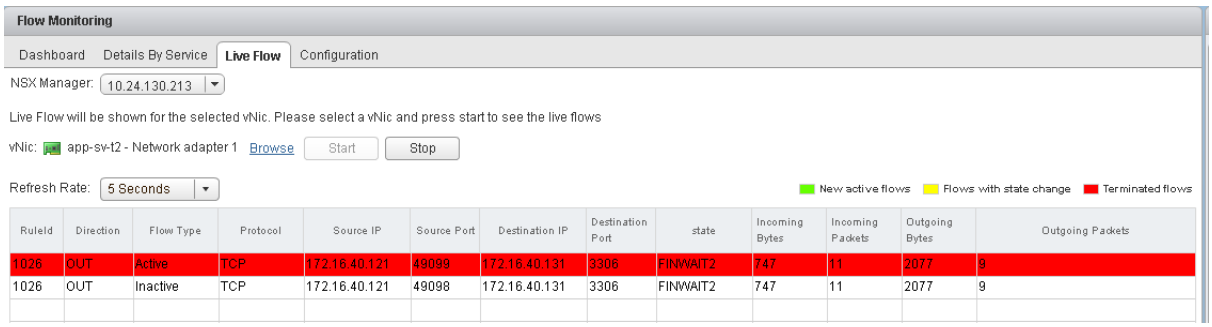
2 Select **Networking & Security** from the left navigation pane and then select **Flow Monitoring**.

3 Click the **Live Flow** tab.

4 Click **Browse** and select a vNIC.

5 Click **Start** to begin viewing live flow.

The page refreshes every 5 seconds. You can select a different frequency from the **Refresh Rate** drop-down.



RuleId	Direction	Flow Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	state	Incoming Bytes	Incoming Packets	Outgoing Bytes	Outgoing Packets
1026	OUT	Active	TCP	172.16.40.121	49099	172.16.40.131	3306	FINWAIT2	747	11	2077	9
1026	OUT	Inactive	TCP	172.16.40.121	49098	172.16.40.131	3306	FINWAIT2	747	11	2077	9

6 Click **Stop** when your debugging or troubleshooting is done to avoid affecting the performance of NSX Manager or the selected virtual machine.

Add or Edit a Firewall Rule from the Flow Monitoring Report

By drilling down into the traffic data, you can evaluate the use of your resources and send session information to Distributed Firewall to create a new allow or block rule at any level.

Procedure

1 Log in to the vSphere Web Client.

2 Select **Networking & Security** from the left navigation pane and then select **Flow Monitoring**.

3 Click the **Details by Service** tab.

4 Click a service to view the traffic flow for it.

Depending on the selected tab, rules that allowed or denied traffic for this service are displayed.

5 Click a rule ID to view rule details.

6 Do one of the following:

- To edit a rule:
  1 Click **Edit Rule** in the **Actions** column.
  2 Change the name, action, or comments for the rule.

3 Click OK.

- To add a rule:

  1 Click **Add Rule** in the **Actions** column.

  2 Complete the form to add a rule. For information on completing the firewall rule form, see "Add a Firewall Rule," on page 43.

  3 Click **OK**.

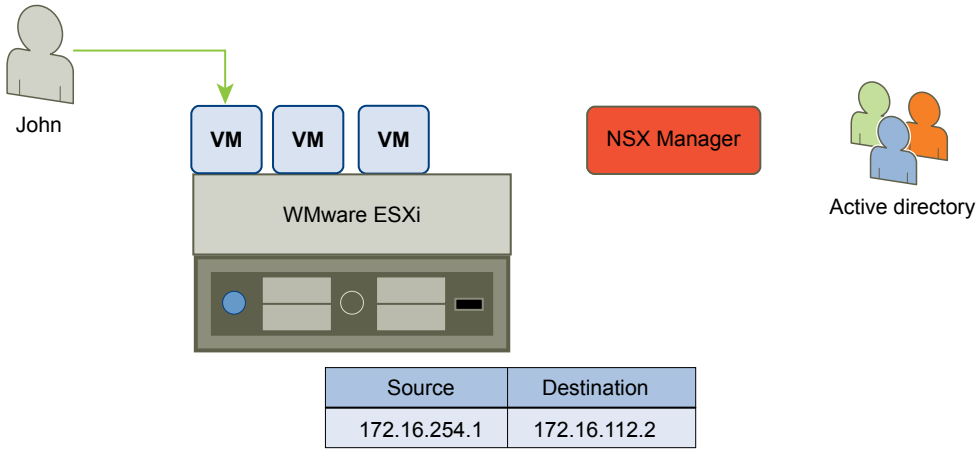
  The rule is added at the top of the firewall rule section.

Activity Monitoring

Activity Monitoring provides visibility into your virtual network to ensure that security policies at your organization are being enforced correctly.

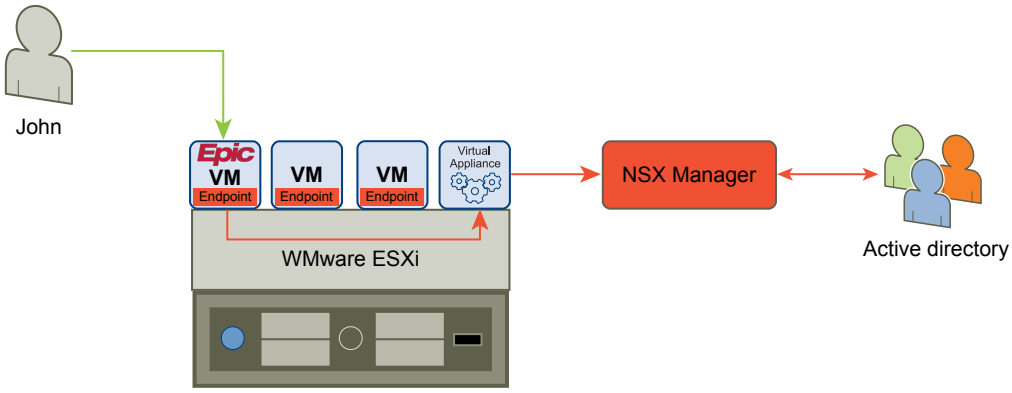
A Security policy may mandate who is allowed access to what applications. The Cloud administrator can generate Activity Monitoring reports to see if the IP based firewall rule that they set is doing the intended work. By providing user and application level detail, Activity Monitoring translates high level security policies to low level IP address and network based implementation.

Figure 14-2. Your virtual environment today



Once you enable data collection for Activity Monitoring, you can run reports to view inbound traffic (such as virtual machines being accessed by users) as well as outbound traffic (resource utilization, interaction between inventory containers, and AD groups that accessed a server).

Figure 14-3. Your virtual environment with Activity Monitoring



User	AD group	App name	Originating VM name	Destination VM name	Source IP	Destination IP
John	Doctors	Epic.exe	DoctorsWS13	EpicSVR3	172.16.254.1	172.16.112.2

Activity Monitoring Scenarios

This section describes some hypothetical scenarios for Activity Monitoring.

User Access to Applications

Our hypothetical company, ACME Enterprise, only permits approved users to access specific applications on corporate assets.

Their security policy mandates are:

- Allow only authorized users to access critical business applications
- Allow only authorized applications on corporate servers
- Allow access to only required ports from specific networks

Based on the above, they need controlled access for employees based on user identity to safeguard corporate assets. As a starting point, the security operator at ACME Enterprise needs to be able to verify that only administrative access is allowed to the MS SQL servers.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then **Activity Monitoring**.

3 Click the **Inbound Activity** tab.

4 Leave **Outbound from** value as **All Observed AD Groups** to see access from any and all employees.

5 In **Where destination virtual machine**, select **includes**.

6 Click the link next to **And where destination virtual machine** and select the MS SQL servers.

7 Click **Search**.

The search results show that only administrative users are accessing the MS SQL servers. Notice that are no groups (such as Finance or HR) accessing these servers.

8 We can now invert this query by setting the **Outbound from** value to HR and Finance AD groups.

9 Click **Search**.

No records are displayed, confirming that no users from either of these groups can access MS SQL servers.

Applications on Datacenter

As part of their security policies, ACME Enterprise needs Visibility into all data center applications. This can help Identify rogue applications that either capture confidential information or siphon sensitive data to external sources.

John, Cloud Administrator at ACME Enterprise, wants to confirm that access to the share point server is only through Internet Explorer and no rogue application (such as FTP or RDP) can access this server.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then **Activity Monitoring**.

3 Click the **VM Activity** tab.

4 Leave **Where source** value as **All observed virtual machines** to capture traffic originating from all virtual machines in the datacenter.

5 In **Where destination**, select **includes**.

6 Click the link next to **And where destination virtual machine** and select the share point server.

7 Click **Search**.

The **Outbound App** column in the search results show that all access to the share point server was only through Internet Explorer. The relatively homogenous search results indicate that there is a firewall rule applied to this share point server preventing all other access methods.

Also note that the search results display the source user of the observed traffic rather than the source group. Clicking the arrow in the search result displays details about the source user such as the AD group to which the user belongs.

Verify Open Ports

Once John Admin knows that the ACME Enterprise share point server is being accessed only by authorized applications, he can ensure that the company allows only required ports to be open based on expected use.

Prerequisites

In the "Applications on Datacenter," on page 188 scenario, John Admin had observed traffic to the ACME Enterprise share point server. He now wants to ensure that all access from the share point server to the MSSQL server is through expected protocols and applications.

Procedure

1 Click the **Go Home** icon.

2 Click **vCenter Home** and then click **Virtual Machines**.

3 Select **win_sharepoint** and then click the **Monitor** tab.

4 Click **Activity Monitoring**.

5 In **Where destination**, select **win2K-MSSQL**.

6 Click **Search**.

Search results show traffic from the share point server to the MSSQL server. The **User** and **Outbound App** columns show that only systems processes are connecting to the MSSQL server, which is what John expected to see.

The **Inbound Port** and **App** columns show that all access is to the MSSQL server running on the destination server.

Since there are too many records in the search results for John to analyze in a web browser, he can export all the entire result set and save the file in a CSV format by clicking the  icon on the bottom right side of the page.

Enable Data Collection

You must enable data collection for one or more virtual machines on a vCenter Server before running an Activity Monitoring report. Before running a report, ensure that the enabled virtual machines are active and are generating network traffic.

You should also register NSX Manager with the AD Domain Controller. See "Register a Windows Domain with NSX Manager," on page 164.

Note that only active connections are tracked by Activity Monitoring. Virtual machine traffic blocked by firewall rules at the vNIC level is not reflected in reports.

Enable Data Collection on a Single Virtual Machine

You must enable data collection at least five minutes before running an Activity Monitoring report.

Prerequisites

Procedure

1 Log in to the vSphere Web Client.

2 Click **vCenter** and then click **VMs and Templates**.

3 Select a virtual machine from the left inventory panel.

4 Click the **Manage** tab and then click the **Settings** tab.

5 Click **NSX Activity Monitoring** from the left panel.

6 Click **Edit**.

7 In the Edit NSX Activity Monitoring Data Collection Settings dialog box, click **Yes**.

Enable Data Collection for Multiple Virtual Machines

The Activity Monitoring Data Collection security group is a pre-defined security group. You can add multiple virtual machines to this security group at a time, and data collection is enabled on all of these virtual machines.

You must enable data collection at least five minutes before running an Activity Monitoring report.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Groups** tab.

4 Select the Activity Monitoring Data Collection security group and click the **Edit** () icon.

5 Follow the wizard to add virtual machines to the security group.

Data collection is enabled on all virtual machines you added to this security group, and disabled on any virtual machines you excluded from the security group.

View Virtual Machine Activity Report

You can view traffic to or from a virtual machine or a set of virtual machines in your environment.

You can either do a quick query using the default search criteria by clicking **Search**, or tailor the query according to your requirements.

Prerequisites

- Either Guest Introspection must be installed in your environment or a domain must be registered with NSX Manager. For information on Endpoint installation, see *NSX Installation and Upgrade Guide*. For information on domain registration, see "Register a Windows Domain with NSX Manager," on page 164.
- Data collection must be enabled on one or more virtual machines.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then **Activity Monitoring**.

3 Click the **VM Activity** tab.

4 Click the link next to **Where source**. Select the virtual machines for which you want to view outbound traffic. Indicate whether you want to include or exclude the selected virtual machine(s) from the report.

5 Click the link next to **Where destination**. Select the virtual machines for which you want to view inbound traffic. Indicate whether you want to include or exclude the selected virtual machine(s) from the report.

6 Click the **During period** ( ) icon and select the time period for the search.

7 Click **Search**.

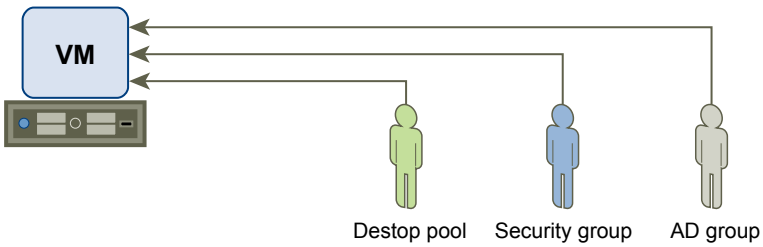
Search results filtered by the specified criterion are displayed. Click a row to view detailed information about the user for that row.

You can export a specific record or all records on this page and save them to a directory in a .csv format by clicking the icon on the bottom right side of the page.

View Inbound Activity

You can view all inbound activity to a server by desktop pool, security group, or AD group.

Figure 14-4. View inbound activity



You can either do a quick query using the default search criteria by clicking **Search**, or tailor the query according to your requirements.

Prerequisites

- Either Guest Introspection must be installed in your environment or a domain must be registered with NSX Manager. For information on Endpoint installation, see *NSX Installation and Upgrade Guide*. For information on domain registration, see "Register a Windows Domain with NSX Manager," on page 164.
- Data collection must be enabled on one or more virtual machines.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then **Activity Monitoring**.

3 Click the **Inbound Activity** tab.

4 Click the link next to **Originating from**.

5 Select the type of user group that you want to view activity for.

6 In **Filter type**, select one or more group and click OK.

7 In **Where destination virtual machine**, select **includes** or **excludes** to indicate whether the selected virtual machines should be included in or excluded from the search.

8 Click the link next to **And where destination virtual machine**.

9 Select one or more virtual machine and click **OK**.

10 In **And where destination application**, select **includes** or **excludes** to indicate whether the selected applications should be included in or excluded from the search.

11 Click the link next to **And where destination application**.

12 Select one or more application and click **OK**.

13 Click the **During period** ( ) icon and select the time period for the search.

14 Click **Search**.

Search results filtered by the specified criterion are displayed. Click anywhere in the results table to view information about the users that accessed the specified virtual machines and applications.

You can export a specific record or all records on this page and save them to a directory in a .csv format by clicking the icon on the bottom right side of the page.

View Outbound Activity

You can view what applications are being run by a security group or desktop pool and then drill down into the report to find out which client applications are making outbound connections by a particular group of users. You can also discover all user groups and users who are accessing a particular application, which can help you determine if you need to adjust identity firewall in your environment.

Figure 14-5. VIew Outbound activity

Prerequisites

- Either Guest Introspection must be installed in your environment or a domain must be registered with NSX Manager. For information on Endpoint installation, see *NSX Installation and Upgrade Guide*. For information on domain registration, see "Register a Windows Domain with NSX Manager," on page 164.
- Data collection must be enabled on one or more virtual machines.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then **Activity Monitoring**.

3 Ensure that the **Outbound Activity** tab is selected in the left pane.

4 Click the link next to **Originating from**.

All groups discovered through guest introspection are displayed.

5 Select the type of user group that you want to view resource utilization for.

6 In **Filter**, select one or more group and click **OK**.

7 In **Where application**, select **includes** or **excludes** to indicate whether the selected application should be included in or excluded from the search.

8 Click the link next to **Where application**.

9 Select one or more application and click **OK**.

10 In **And where destination**, select **includes** or **excludes** to indicate whether the selected virtual machines should be included in or excluded from the search.

11 Click the link next to **And where destination**.

12 Select one or more virtual machine and click **OK**.

13 Click the **During period** () icon and select the time period for the search.

14 Click **Search**.

Scroll to the right to see all the information displayed.

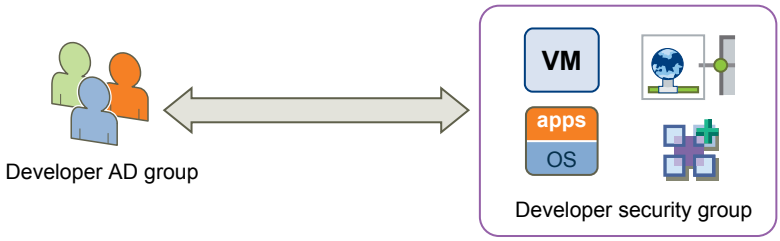
Search results filtered by the specified criterion are displayed. Click a row to view information about users within that AD group that used the specified application to access the specified virtual machines.

You can export a specific record or all records on this page and save them to a directory in a .csv format by clicking the  icon on the bottom right side of the page.

View Interaction between Inventory Containers

You can view the traffic passing between defined containers such as AD groups, security groups and/or desktop pools. This can help you identify and configure access to shared services and to resolve mis-configured relationships between Inventory container definitions, desktop pools and AD groups.

Figure 14-6. Interaction between containers



You can either do a quick query using the default search criteria by clicking **Search**, or tailor the query according to your requirements.

Prerequisites

- Either Guest Introspection must be installed in your environment or a domain must be registered with NSX Manager. For information on Endpoint installation, see *NSX Installation and Upgrade Guide*. For information on domain registration, see "Register a Windows Domain with NSX Manager," on page 164.
- Data collection must be enabled on one or more virtual machines.

Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then **Activity Monitoring**.
3. Select the **Inter Container Interaction** tab in the left pane.
4. Click the link next to **Originating from**.

   All groups discovered through guest introspection are displayed.
5. Select the type of user group that you want to view resource utilization for.
6. In **Filter**, select one or more group and click **OK**.
7. In **Where the destination is**, select **is** or **is not** to indicate whether the selected group should be included in or excluded from the search.
8. Click the link next to **Where the destination is**.
9. Select the group type.
10. In **Filter**, select one or more group and click **OK**.
11. Click the **During period** ( ) icon and select the time period for the search.
12. Click **Search**.

Search results filtered by the specified criterion are displayed. Click in a row to view information about the users that accessed the specified containers.

You can export a specific record or all records on this page and save them to a directory in a .csv format by clicking the icon on the bottom right side of the page.

Example: Interaction between Inventory Containers Query

- Verify allowed communication

  If you have defined containers in your vCenter inventory and then added a rule to allow communication between these containers, you can verify that the rule is working by running this query with the two containers specified in the **Originating from** and **Where the destination is** fields.

- Verify denied communication

  If you have defined containers in your vCenter inventory and then added a rule to deny communication between these containers, you can verify that the rule is working by running this query with the two containers specified in the **Originating from** and **Where the destination is** fields.

- Verify denied intra-container communication

  If you have implemented a policy that does not allow members of a container communicating with other members of the same container, you can run this query to verify that the policy works. Select the container in both **Originating from** and **Where the destination is** fields.

- Eliminate unnecessary access

  Suppose you have defined containers in your vCenter inventory and then added a rule to allow communication between these containers. There may be members in either container that do not interact with the other container at all. You may then choose to remove these members from the appropriate container to optimize security control. To retrieve such a list, select the appropriate containers in both **Originating from** and **Where the destination is** fields. Select **is not** next to the **Where the destination is** field.

View Outbound AD Group Activity

You can view the traffic between members of defined Active Directory groups and can use this data to fine-tune your firewall rules.

You can either do a quick query using the default search criteria by clicking **Search**, or tailor the query according to your requirements.

Prerequisites

- Either Guest Introspection must be installed in your environment or a domain must be registered with NSX Manager. For information on Endpoint installation, see *NSX Installation and Upgrade Guide*. For information on domain registration, see "Register a Windows Domain with NSX Manager," on page 164.
- Data collection must be enabled on one or more virtual machines.

Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then **Activity Monitoring**.
3. Select the **AD Groups & Containers** tab in the left pane.
4. Click the link next to **Originating from**.

   All groups discovered through guest introspection are displayed.
5. Select the type of user group that you want to include in the search.
6. In **Filter**, select one or more group and click **OK**.
7. In **Where AD Group**, select **includes** or **excludes** to indicate whether the selected AD group should be included in or excluded from the search.

8 Click the link next to **Where AD Group**.

9 Select one or more AD groups and click **OK**.

10 Click the **During period** ( ) icon and select the time period for the search.

11 Click **Search**.

Search results filtered by the specified criterion are displayed. Click in a row to view information about the members of the specified AD group that are accessing network resources from within the specified security group or desktop pool.

You can export a specific record or all records on this page and save them to a directory in a .csv format by clicking the icon on the bottom right side of the page.

Override Data Collection

In case of an emergency such as a network overload, you can turn off data collection at a global level. This overrides all other data collection settings.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then **Activity Monitoring**.

3 Click the **Settings** tab.

4 Select the vCenter Server for which you want to overwrite data collection.

5 Click **Edit**.

6 De-select **Collect reporting data**.

7 Click **OK**.

Guest Introspection Events and Alarms

Guest Introspection offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance delivered by VMware partners. Since the secure virtual appliance (unlike a guest virtual machine) doesn't go offline, it can continuously update antivirus signatures thereby giving uninterrupted protection to the virtual machines on the host. Also, new virtual machines (or existing virtual machines that went offline) are immediately protected with the most current antivirus signatures when they come online.

Guest Introspection health status is conveyed by using alarms that show in red on the vCenter Server console. In addition, more status information can be gathered by looking at the event logs.

Important Your vCenter Server must be correctly configured for Guest Introspection security:

- Not all guest operating systems are supported by Guest Introspection. Virtual machines with non-supported operating systems are not protected by the security solution.
- All hosts in a resource pool containing protected virtual machines must be prepared for Guest Introspection so that virtual machines continue to be protected as they are vMotioned from one ESX host to another within the resource pool.

View Guest Introspection Status

Monitoring a Guest Introspection instance involves checking for status coming from the Guest Introspection components: the security virtual machine (SVM), the ESX host-resident Guest Introspection module, and the protected virtual machine-resident thin agent.

Procedure

1 In the vSphere Web Client, click **vCenter**, and then click **Datacenters**.

2 In the **Name** column, click a datacenter.

3 Click **Monitor** and then click **Endpoint**.

The Guest Introspection Health and Alarms page displays the health of the objects under the datacenter you selected, and the active alarms. Health status changes are reflected within a minute of the actual occurrence of the event that triggered the change.

Guest Introspection Alarms

Alarms signal the vCenter Server administrator about Guest Introspection events that require attention. Alarms are automatically cancelled in case the alarm state is no longer present.

vCenter Server alarms can be displayed without a custom vSphere plug-in. See the *vCenter Server Administration Guide* on events and alarms.

Upon registering as a vCenter Server extension, NSX Manager defines the rules that create and remove alarms, based on events coming from the three Guest Introspection components: SVM, Guest Introspection module, and thin agent. Rules can be customized. For instructions on how to create new custom rules for alarms, see the vCenter Server documentation. In some cases, there are multiple possible causes for the alarm. The tables that follow list the possible causes and the corresponding actions you might want to take for remediation.

Host Alarms

Host alarms are generated by events affecting the health status of the Guest Introspection module.

Table 14-5. Errors (Marked Red)

Possible Cause	Action
The Guest Introspection module has been installed on the host, but is no longer reporting status to the NSX Manager.	1 Ensure that Guest Introspection is running by logging in to the host and typing the command `/etc/init.d/vShield-Endpoint-Mux start`. 2 Ensure that the network is configured properly so that Guest Introspection can connect to NSX Manager. 3 Reboot the NSX Manager.

SVM Alarms

SVM alarms are generated by events affecting the health status of the SVM.

Table 14-6. Red SVM Alarms

Problem	Action
There is a protocol version mismatch with the Guest Introspection module	Ensure that the Guest Introspection module and SVM have a protocol that is compatible with each other.
Guest Introspection could not establish a connection to the SVM	Ensure that the SVM is powered on and that the network is configured properly.
The SVM is not reporting its status even though guests are connected.	Internal error. Contact your VMware support representative.

Guest Introspection Events

Events are used for logging and auditing conditions inside the Guest Introspection-based security system.

Events can be displayed without a custom vSphere plug-in. See the *vCenter Server Administration Guide* on events and alarms.

Events are the basis for alarms that are generated. Upon registering as a vCenter Server extension, the NSX Manager defines the rules that create and remove alarms.

Common arguments for all events are the event time stamp and the NSX Manager `event_id`.

The following table lists Guest Introspection events reported by the SVM and the NSX Manager.

Table 14-7. Guest Introspection Events

Description	Severity	VC Arguments
Guest Introspection solution *SolutionName* enabled. Supporting version *versionNumber* of the VFile protocol.	info	timestamp
ESX module enabled.	info	timestamp
ESX module uninstalled.	info	timestamp
The NSX Manager has lost connection with the ESX module.	info	timestamp
Guest Introspection solution *SolutionName* was contacted by a non-compatible version of the ESX module.	error	timestamp, solution version, ESX module version
A connection between the ESX module and *SolutionName* failed.	error	timestamp, ESX module version, solution version
Guest Introspection failed to connect to the SVM.	error	timestamp
Guest Introspection lost connection with the SVM.	error	timestamp

Guest Introspection Audit Messages

Audit messages include fatal errors and other important audit messages and are logged to `vmware.log`.

The following conditions are logged as AUDIT messages:

- Thin agent initialization success (and version number.)
- Thin agent initialization failure.
- Established first time communication with SVM.

- Failure to establish communication with SVM (when first such failure occurs).

Generated log messages have the following substrings near the beginning of each log message: `vf-AUDIT`, `vf-ERROR`, `vf-WARN`, `vf-INFO`, `vf-DEBUG`.

NSX Edge VPN Configuration Examples

15

This scenario contains configuration examples for a basic point-to-point IPSEC VPN connection between anNSX Edge and a Cisco or WatchGuard VPN on the other end.

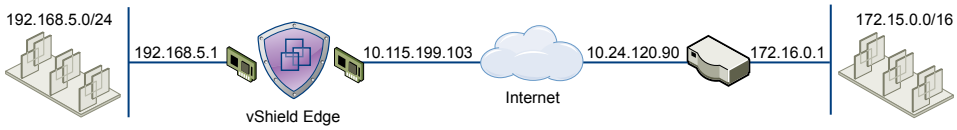
For this scenario,NSX Edge connects the internal network 192.0.2.0/24 to the internet. NSX Edge interfaces are configured as follows:

- Uplink interface: 198.51.100.1
- Internal interface: 192.0.2.1

The remote gateway connects the 172.16.0.0/16 internal network to the internet. The remote gateway interfaces are configured as follows:

- Uplink interface: 10.24.120.90/24
- Internal interface: 172.16.0.1/16

Figure 15-1. NSX Edge connecting to a remote VPN gateway



NOTE For NSX Edge to NSX Edge IPSEC tunnels, you can use the same scenario by setting up the second NSX Edge as the remote gateway.

This chapter includes the following topics:

- "Terminology," on page 200
- "IKE Phase 1 and Phase 2," on page 200
- "Configuring IPSec VPN Service Example," on page 202
- "Using a Cisco 2821 Integrated Services Router," on page 203
- "Using a Cisco ASA 5510," on page 206
- "Configuring a WatchGuard Firebox X500," on page 208
- "Troubleshooting NSX Edge Configuration Example," on page 209

Terminology

IPSec is a framework of open standards. There are many technical terms in the logs of the NSX Edge and other VPN appliances that you can use to troubleshoot the IPSEC VPN.

These are some of the standards you may encounter:

- ISAKMP (Internet Security Association and Key Management Protocol) is a protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent.
- Oakley is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie-Hellman key exchange algorithm.
- IKE (Internet Key Exchange) is a combination of ISAKMP framework and Oakley. NSX Edge provides IKEv2.
- Diffie-Hellman (DH) key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. VSE supports DH group 2 (1024 bits) and group 5 (1536 bits).

IKE Phase 1 and Phase 2

IKE is a standard method used to arrange secure, authenticated communications.

Phase 1 Parameters

Phase 1 sets up mutual authentication of the peers, negotiates cryptographic parameters, and creates session keys. The Phase 1 parameters used by NSX Edge are:

- Main mode
- TripleDES / AES [Configurable]
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret [Configurable]
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying
- ISAKMP aggressive mode disabled

Phase 2 Parameters

IKE Phase 2 negotiates an IPSec tunnel by creating keying material for the IPSec tunnel to use (either by using the IKE phase one keys as a base or by performing a new key exchange). The IKE Phase 2 parameters supported by NSX Edge are:

- TripleDES / AES [Will match the Phase 1 setting]
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying

- Selectors for all IP protocols, all ports, between the two networks, using IPv4 subnets

Transaction ModeSamples

NSX Edge supports Main Mode for Phase 1 and Quick Mode for Phase 2.

NSX Edge proposes a policy that requires PSK, 3DES/AES128, sha1, and DH Group 2/5. The peer must accept this policy; otherwise, the negotiation phase fails.

Phase 1: Main Mode Transactions

This example shows an exchange of Phase 1 negotiation initiated from a NSX Edge to a Cisco device.

The following transactions occur in sequence between the NSX Edge and a Cisco VPN device in Main Mode.

1 NSX Edge to Cisco
   - proposal: encrypt 3des-cbc, sha, psk, group5(group2)
   - DPD enabled

2 Cisco to NSX Edge
   - contains proposal chosen by Cisco
   - If the Cisco device does not accept any of the parameters the NSX Edge sent in step one, the Cisco device sends the message with flag NO_PROPOSAL_CHOSEN and terminates the negotiation.

3 NSX Edge to Cisco
   - DH key and nonce

4 Cisco to NSX Edge
   - DH key and nonce

5 NSX Edge to Cisco (Encrypted)
   - include ID (PSK)

6 Cisco to NSX Edge (Encrypted)
   - include ID (PSK)
   - If the Cisco device finds that the PSK doesn't match, the Cisco device sends a message with flag INVALID_ID_INFORMATION; Phase 1 fails.

Phase 2: Quick Mode Transactions

The following transactions occur in sequence between the NSX Edge and a Cisco VPN device in Quick Mode.

1 NSX Edge to Cisco

   NSX Edge proposes Phase 2 policy to the peer. For example:

```
Aug 26 12:16:09 weiqing-desktop
ipsec[5789]:
"s1-c1" #2: initiating Quick Mode
PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
{using isakmp#1 msgid:d20849ac
proposal=3DES(3)_192-SHA1(2)_160
pfsgroup=OAKLEY_GROUP_MODP1024}
```

2 Cisco to NSX Edge

Cisco device sends back NO_PROPOSAL_CHOSEN if it does not find any matching policy for the proposal. Otherwise, the Cisco device sends the set of parameters chosen.

3 NSX Edge to Cisco

To facilitate debugging, you can enable IPSec logging on the NSX Edge and enable crypto debug on Cisco (debug crypto isakmp <level>).

Configuring IPSec VPN Service Example

You must configure VPN parameters and then enable the IPSEC service.

Procedure

1 Configure NSX Edge VPN Parameters Example on page 202

You must configure at least one external IP address on NSX Edge to provide IPSec VPN service.

2 Enable IPSec VPN Service Example on page 203

You must enable the IPSec VPN service for traffic to flow from the local subnet to the peer subnet.

Configure NSX Edge VPN Parameters Example

You must configure at least one external IP address on NSX Edge to provide IPSec VPN service.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click the **VPN** tab.

5 Click **IPSec VPN**.

6 Click the **Add** () icon.

7 Type a name for the IPSec VPN.

8 Type the IP address of the NSX Edge instance in **Local Id**. This will be the peer Id on the remote site.

9 Type the IP address of the local endpoint.

If you are adding an IP to IP tunnel using a pre-shared key, the local Id and local endpoint IP can be the same.

10 Type the subnets to share between the sites in CIDR format. Use a comma separator to type multiple subnets.

11 Type the Peer Id to uniquely identify the peer site. For peers using certificate authentication, this ID must be the common name in the peer's certificate. For PSK peers, this ID can be any string. VMware recommends that you use the public IP address of the VPN or a FQDN for the VPN service as the peer ID

12 Type the IP address of the peer site in Peer Endpoint. If you leave this blank, NSX Edge waits for the peer device to request a connection.

13 Type the internal IP address of the peer subnet in CIDR format. Use a comma separator to type multiple subnets.

14 Select the Encryption Algorithm.

15 In Authentication Method, select one of the following:

Option	Description
PSK (Pre Shared Key)	Indicates that the secret key shared between NSX Edge and the peer site is to be used for authentication. The secret key can be a string with a maximum length of 128 bytes.
Certificate	Indicates that the certificate defined at the global level is to be used for authentication.

16 Type the shared key in if anonymous sites are to connect to the VPN service.

17 Click **Display Shared Key** to display the key on the peer site.

18 In Diffie-Hellman (DH) Group, select the cryptography scheme that will allow the peer site and the NSX Edge to establish a shared secret over an insecure communications channel.

19 Change the MTU threshold if required.

20 Select whether to enable or disable the Perfect Forward Secrecy (PFS) threshold. In IPsec negotiations, Perfect Forward Secrecy (PFS) ensures that each new cryptographic key is unrelated to any previous key.

21 Click **OK**.

NSX Edge creates a tunnel from the local subnet to the peer subnet.

What to do next

Enable the IPSec VPN service.

Enable IPSec VPN Service Example

You must enable the IPSec VPN service for traffic to flow from the local subnet to the peer subnet.

Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click an NSX Edge.

4 Click the **Monitor** tab and then click the **VPN** tab.

5 Click **IPSec VPN**.

6 Click **Enable**.

What to do next

Click **Enable Logging** to log the traffic flow between the local subnet and peer subnet.

Using a Cisco 2821 Integrated Services Router

The following describes configurations performed using Cisco IOS.

Procedure

1 Configure Interfaces and Default Route

```
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
```

```
crypto map MYVPN
!
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 10.24.123.253
```

2 Configure IKE Policy

```
Router# config term
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# encryption 3des
Router(config-isakmp)# group 2
Router(config-isakmp)# hash sha
Router(config-isakmp)# lifetime 28800
Router(config-isakmp)# authentication
     pre-share
Router(config-isakmp)# exit
```

3 Match Each Peer with Its Pre-Shared Secret

```
Router# config term
Router(config)# crypto isakmp key vshield
    address 10.115.199.103
Router(config-isakmp)# exit
```

4 Define the IPSEC Transform

```
Router# config term
Router(config)# crypto ipsec transform-set
     myset esp-3des esp-sha-hmac
Router(config-isakmp)# exit
```

5 Create the IPSEC Access List

```
Router# config term
Enter configuration commands, one per line.
     End with CNTL/Z.
Router(config)# access-list 101 permit ip
     172.16.0.0 0.0.255.255 192.168.5.0 0.0.0.255
Router(config)# exit
```

6 Bind the Policy with a Crypto Map and Label It

In the following example, the crypto map is labeled MYVPN

```
Router# config term
Router(config)# crypto map MYVPN 1
      ipsec-isakmp
% NOTE: This new crypto map will remain
      disabled until a peer and a valid
      access list have been configured.
Router(config-crypto-map)# set transform-set
      myset
Router(config-crypto-map)# set pfs group1
Router(config-crypto-map)# set peer
      10.115.199.103
Router(config-crypto-map)# match address 101
Router(config-crypto-map)# exit
```

Example: Example Configuration

```
router2821#show running-config output
Building configuration...

Current configuration : 1263 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2821
!
boot-start-marker
boot-end-marker
!
! card type command needed for slot 0
! card type command needed for slot 1
enable password cisco
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
ip cef
!no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key vshield address 10.115.199.103
!
crypto ipsec transform-set myset esp-3des
      esp-sha-hmac
!
crypto map MYVPN 1 ipsec-isakmp
set peer 10.115.199.103
set transform-set myset
set pfs group1
match address 101
!
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
crypto map MYVPN
!
```

```
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.24.123.253
!
ip http server
no ip http secure-server
!
access-list 101 permit ip 172.16.0.0
       0.0.255.255 192.168.5.0 0.0.0.255
!
control-plane
!
line con 0
line aux 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
scheduler allocate 20000 1000
!
end
```

Using a Cisco ASA 5510

Use the following output to configure a Cisco ASA 5510.

```
ciscoasa# show running-config output
: Saved
:
ASA Version 8.2(1)18
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
nameif untrusted
security-level 100
ip address 10.24.120.90 255.255.252.0
!
interface Ethernet0/1
nameif trusted
security-level 90
ip address 172.16.0.1 255.255.0.0
!
interface Ethernet0/2
shutdown
no nameif
```

```
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
boot system disk0:/asa821-18-k8.bin
ftp mode passive
access-list ACL1 extended permit ip 172.16.0.0 255.255.0.0
      192.168.5.0 255.255.255.0
access-list ACL1 extended permit ip 192.168.5.0 255.255.255.0
      172.16.0.0 255.255.0.0
access-list 101 extended permit icmp any any
pager lines 24
mtu untrusted 1500
mtu trusted 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any untrusted
icmp permit any trusted
no asdm history enable
arp timeout 14400
access-group 101 in interface untrusted
access-group 101 out interface untrusted
access-group 101 in interface trusted
access-group 101 out interface trusted
route untrusted 10.115.0.0 255.255.0.0 10.24.123.253 1
route untrusted 192.168.5.0 255.255.255.0 10.115.199.103 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
      udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
      mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
      sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
crypto ipsec transform-set MYSET esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto map MYVPN 1 match address ACL1
crypto map MYVPN 1 set pfs
crypto map MYVPN 1 set peer 10.115.199.103
```

```
crypto map MYVPN 1 set transform-set MYSET
crypto map MYVPN interface untrusted
crypto isakmp enable untrusted
crypto isakmp policy 1
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
telnet 10.0.0.0 255.0.0.0 untrusted
telnet timeout 5
ssh timeout 5
console timeout 0
no threat-detection basic-threat
no threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password f3UhLvUj1QsXsuK7 encrypted
tunnel-group 10.115.199.103 type ipsec-l2l
tunnel-group 10.115.199.103 ipsec-attributes
pre-shared-key *
!
!
prompt hostname context
Cryptochecksum:29c3cc49460831ff6c070671098085a9
: end
```

Configuring a WatchGuard Firebox X500

You can configure your WatchGuard Firebox X500 as a remote gateway.

NOTE Refer to your WatchGuard Firebox documentation for exact steps.

Procedure

1 In Firebox System Manager, select **Tools > Policy Manager** > .

2 In Policy Manager, select **Network > Configuration**.

3 Configure the interfaces and click **OK**.

4 (Optional) Select **Network > Routes** to configure a default route.

5 Select **Network > Branch Office VPN > Manual IPSec** to configure the remote gateway.

6 In the IPSec Configuration dialog box, click **Gateways** to configure the IPSEC Remote Gateway.

7 In the IPSec Configuration dialog box, click **Tunnels** to configure a tunnel.

8 In the IPSec Configuration dialog box, click **Add** to add a routing policy.

9 Click **Close**.

10 Confirm that the tunnel is up.

Troubleshooting NSX Edge Configuration Example

Use this information to help you troubleshoot negotiation problems with your setup.

Successful Negotiation (both Phase 1 and Phase 2)

The following examples display a successful negotiating result between NSX Edge and a Cisco device.

NSX Edge

From the NSX Edge command line interface (ipsec auto -status, part of show service ipsec command):

```
000 #2: "s1-c1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established);
      EVENT_SA_REPLACE in 2430s; newest IPSEC; eroute owner; isakmp#1; idle;
      import:admin initiate
000 #2: "s1-c1" esp.f5f6877d@10.20.131.62 esp.7aaf335f@10.20.129.80
      tun.0@10.20.131.62 tun.0@10.20.129.80 ref=0 refhim=4294901761
000 #1: "s1-c1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in
      27623s; newest ISAKMP; lastdpd=0s(seq in:0 out:0); idle;
      import:admin initiate
```

Cisco

```
ciscoasa# show crypto isakmp sa detail

    Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

    IKE Peer: 10.20.129.80
    Type : L2L        Role    : responder
    Rekey : no        State   : MM_ACTIVE
    Encrypt : 3des    Hash    : SHA
    Auth : preshared  Lifetime: 28800
    Lifetime Remaining: 28379
```

Phase 1 Policy Not Matching

The following lists Phase 1 Policy Not Matching Error logs.

NSX Edge

NSX Edge hangs in STATE_MAIN_I1 state. Look in /var/log/messages for information showing that the peer sent back an IKE message with "NO_PROPOSAL_CHOSEN" set.

```
000 #1: "s1-c1":500 STATE_MAIN_I1 (sent MI1,
      expecting MR1); EVENT_RETRANSMIT in 7s; nodpd; idle;
      import:admin initiate
000 #1: pending Phase 2 for "s1-c1" replacing #0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | ***parse ISAKMP Notification Payload:
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |    next payload type: ISAKMP_NEXT_NONE
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |    length: 96
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
```

```
      |    DOI: ISAKMP_DOI_IPSEC
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |    protocol ID: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |    SPI size: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |    Notify Message Type: NO_PROPOSAL_CHOSEN
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      "s1-c1" #1: ignoring informational payload,
       type NO_PROPOSAL_CHOSEN msgid=00000000
```

Cisco

If debug crypto is enabled, an error message is printed to show that no proposals were accepted.

```
ciscoasa# Aug 26 18:17:27 [IKEv1]:
      IP = 10.20.129.80, IKE_DECODE RECEIVED
      Message (msgid=0) with payloads : HDR + SA (1)
      + VENDOR (13) + VENDOR (13) + NONE (0) total length : 148
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
      processing SA payload
Aug 26 18:17:27 [IKEv1]: Phase 1 failure:  Mismatched attribute
      types for class Group Description:  Rcv'd: Group 5
      Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: Phase 1 failure:  Mismatched attribute
      types for class Group Description:  Rcv'd: Group 5
      Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
      Message (msgid=0) with payloads : HDR + NOTIFY (11)
      + NONE (0) total length : 124
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
      All SA proposals found unacceptable
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, Error processing
      payload: Payload ID: 1
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE MM Responder
      FSM error history (struct &0xd8355a60)  <state>, <event>:
      MM_DONE, EV_ERROR-->MM_START, EV_RCV_MSG-->MM_START,
      EV_START_MM-->MM_START, EV_START_MM-->MM_START,
      EV_START_MM-->MM_START, EV_START_MM-->MM_START,
      EV_START_MM-->MM_START, EV_START_MM
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE SA
      MM:9e0e4511 terminating:  flags 0x01000002, refcnt 0,
      tuncnt 0
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, sending
      delete/delete with reason message
```

Phase 2 Not Matching

The following lists Phase 2 Policy Not Matching Error logs.

NSX Edge

NSX Edge hangs at STATE_QUICK_I1. A log message shows that the peer sent a NO_PROPOSAL_CHOSEN message.

```
000 #2: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
      QR1); EVENT_RETRANSMIT in 11s; lastdpd=-1s(seq in:0 out:0);
      idle; import:admin initiate
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | got payload
```

```
      0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | ***parse
      ISAKMP Notification Payload:
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    next payload
      type: ISAKMP_NEXT_NONE
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    length: 32
Aug 26 12:33:54 weiqing-desktop ipsec[6933]:
      |    DOI: ISAKMP_DOI_IPSEC
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    protocol ID: 3
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    SPI size: 16
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    Notify Message
      Type: NO_PROPOSAL_CHOSEN
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: "s1-c1" #3:
      ignoring informational payload, type NO_PROPOSAL_CHOSEN
      msgid=00000000
```

Cisco

Debug message show that Phase 1 is completed, but Phase 2 failed because of policy negotiation failure.

```
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80,
      IP = 10.20.129.80, PHASE 1 COMPLETED
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, Keep-alive type
      for this connection: DPD
Aug 26 16:03:49 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, Starting P1 rekey timer: 21600 seconds
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, IKE_DECODE RECEIVED
      Message (msgid=b2cdcb13) with payloads : HDR + HASH (8)
      + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE (0)
      total length : 288
.
.
.
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
      Session is being torn down. Reason: Phase 2 Mismatch
```

PFS Mismatch

The following lists PFS Mismatch Error logs.

NSX Edge

PFS is negotiated as part of Phase 2. If PFS does not match, the behavior is similar to the failure case described in "Phase 2 Not Matching," on page 210.

```
000 #4: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
      QR1); EVENT_RETRANSMIT in 8s; lastdpd=-1s(seq in:0 out:0);
      idle; import:admin initiate
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | got payload 0x800
      (ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      | ***parse ISAKMP Notification Payload:
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    next payload
      type: ISAKMP_NEXT_NONE
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    length: 32
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      |    DOI: ISAKMP_DOI_IPSEC
```

```
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    protocol ID: 3
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    SPI size: 16
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    Notify Message
      Type: NO_PROPOSAL_CHOSEN
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: "s1-c1" #1: ignoring
      informational payload, type NO_PROPOSAL_CHOSEN
      msgid=00000000
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  fa 16 b3 e5
      91 a9 b0 02  a3 30 e1 d9  6e 5a 13 d4
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  93 e5 e4 d7
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      | processing informational NO_PROPOSAL_CHOSEN (14)
```

Cisco

```
<BS>Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, sending delete/delete with
      reason message
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing IKE delete payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing qm hash payload
Aug 26 19:00:26 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
      Message (msgid=19eb1e59) with payloads : HDR + HASH (8)
      + DELETE (12) + NONE (0) total length : 80
Aug 26 19:00:26 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
      Session is being torn down. Reason: Phase 2 Mismatch
```

PSK not Matching

The following lists PSK Not Matching Error logs

NSX Edge

PSK is negotiated in the last round of Phase 1. If PSK negotiation fails, NSX Edge state is STATE_MAIN_I4. The peer sends a message containing INVALID_ID_INFORMATION.

```
Aug 26 11:55:55 weiqing-desktop ipsec[3855]:
      "s1-c1" #1: transition from state STATE_MAIN_I3 to
      state STATE_MAIN_I4
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
      STATE_MAIN_I4: ISAKMP SA established
      {auth=OAKLEY_PRESHARED_KEY
      cipher=oakley_3des_cbc_192 prf=oakley_sha group=modp1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1: Dead Peer
      Detection (RFC 3706): enabled
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #2:
      initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
      {using isakmp#1 msgid:e8add10e proposal=3DES(3)_192-SHA1(2)_160
```

```
      pfsgroup=OAKLEY_GROUP_MODP1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
      ignoring informational payload, type INVALID_ID_INFORMATION
      msgid=00000000
```

Cisco

```
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191,
      IKE_DECODE SENDING Message (msgid=0) with payloads : HDR
      + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
      + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130)
      + NONE (0) total length : 304
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
      IP = 10.115.199.191, Received encrypted Oakley Main Mode
      packet with invalid payloads, MessID = 0
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191, IKE_DECODE SENDING
      Message (msgid=0) with payloads : HDR + NOTIFY (11)
      + NONE (0) total length : 80
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
      IP = 10.115.199.191, ERROR, had problems decrypting
      packet, probably due to mismatched pre-shared key.
      Aborting
```

Packet Capture for a Successful Negotiation

The following lists a packet capture session for a successful negotiation between NSX Edge and a Cisco device.

```
No.     Time        Source        Destination   Protocol Info
9203    768.394800  10.20.129.80  10.20.131.62  ISAKMP  Identity Protection
                                                        (Main Mode)
Frame 9203 (190 bytes on wire, 190 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 0000000000000000
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 148
  Security Association payload
    Next payload: Vendor ID (13)
    Payload length: 84
    Domain of interpretation: IPSEC (1)
    Situation: IDENTITY (1)
    Proposal payload # 0
      Next payload: NONE (0)
      Payload length: 72
      Proposal number: 0
      Protocol ID: ISAKMP (1)
```

```
      SPI Size: 0
      Proposal transforms: 2
      Transform payload # 0
         Next payload: Transform (3)
         Payload length: 32
         Transform number: 0
         Transform ID: KEY_IKE (1)
         Life-Type (11): Seconds (1)
         Life-Duration (12): Duration-Value (28800)
         Encryption-Algorithm (1): 3DES-CBC (5)
         Hash-Algorithm (2): SHA (2)
         Authentication-Method (3): PSK (1)
         Group-Description (4): 1536 bit MODP group (5)
      Transform payload # 1
         Next payload: NONE (0)
         Payload length: 32
         Transform number: 1
         Transform ID: KEY_IKE (1)
         Life-Type (11): Seconds (1)
         Life-Duration (12): Duration-Value (28800)
         Encryption-Algorithm (1): 3DES-CBC (5)
         Hash-Algorithm (2): SHA (2)
         Authentication-Method (3): PSK (1)
         Group-Description (4): Alternate 1024-bit MODP group (2)
  Vendor ID: 4F456C6A405D72544D42754D
    Next payload: Vendor ID (13)
    Payload length: 16
    Vendor ID: 4F456C6A405D72544D42754D
  Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)
    Next payload: NONE (0)
    Payload length: 20
    Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)

No.     Time        Source        Destination   Protocol Info
9204    768.395550  10.20.131.62  10.20.129.80  ISAKMP Identity Protection
                                                       (Main Mode)

Frame 9204 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 104
  Security Association payload
    Next payload: Vendor ID (13)
    Payload length: 52
```

```
    Domain of interpretation: IPSEC (1)
    Situation: IDENTITY (1)
    Proposal payload # 1
      Next payload: NONE (0)
      Payload length: 40
      Proposal number: 1
      Protocol ID: ISAKMP (1)
      SPI Size: 0
      Proposal transforms: 1
      Transform payload # 1
         Next payload: NONE (0)
         Payload length: 32
         Transform number: 1
         Transform ID: KEY_IKE (1)
         Encryption-Algorithm (1): 3DES-CBC (5)
         Hash-Algorithm (2): SHA (2)
         Group-Description (4): Alternate 1024-bit MODP group (2)
         Authentication-Method (3): PSK (1)
         Life-Type (11): Seconds (1)
         Life-Duration (12): Duration-Value (28800)
  Vendor ID: Microsoft L2TP/IPSec VPN Client
    Next payload: NONE (0)
    Payload length: 24
    Vendor ID: Microsoft L2TP/IPSec VPN Client

No.     Time        Source        Destination   Protocol Info
9205    768.399599  10.20.129.80  10.20.131.62  ISAKMP Identity Protection
                                                        (Main Mode)

Frame 9205 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 180
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: NONE (0)
    Payload length: 20
    Nonce Data


No.     Time        Source        Destination   Protocol Info
```

```
9206    768.401192  10.20.131.62  10.20.129.80  ISAKMP Identity Protection
                                                          (Main Mode)
Frame 9206 (298 bytes on wire, 298 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 256
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: Vendor ID (13)
    Payload length: 24
    Nonce Data
  Vendor ID: CISCO-UNITY-1.0
    Next payload: Vendor ID (13)
    Payload length: 20
    Vendor ID: CISCO-UNITY-1.0
  Vendor ID: draft-beaulieu-ike-xauth-02.txt
    Next payload: Vendor ID (13)
    Payload length: 12
    Vendor ID: draft-beaulieu-ike-xauth-02.txt
  Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
    Next payload: Vendor ID (13)
    Payload length: 20
    Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
  Vendor ID: CISCO-CONCENTRATOR
    Next payload: NONE (0)
    Payload length: 20
    Vendor ID: CISCO-CONCENTRATOR

No.     Time        Source        Destination   Protocol Info
9207    768.404990  10.20.129.80  10.20.131.62  ISAKMP Identity Protection
                                                          (Main Mode)

Frame 9207 (110 bytes on wire, 110 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
```

```
  Next payload: Identification (5)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x01
  Message ID: 0x00000000
  Length: 68
  Encrypted payload (40 bytes)

No.     Time        Source        Destination   Protocol Info
9208    768.405921  10.20.131.62  10.20.129.80  ISAKMP   Identity Protection
                                                          (Main Mode)
Frame 9208 (126 bytes on wire, 126 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Identification (5)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x01
  Message ID: 0x00000000
  Length: 84
  Encrypted payload (56 bytes)

No.     Time        Source        Destination   Protocol Info
9209    768.409799  10.20.129.80  10.20.131.62  ISAKMP   Quick Mode

Frame 9209 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 292
  Encrypted payload (264 bytes)

No.     Time        Source        Destination   Protocol Info
9210    768.411797  10.20.131.62  10.20.129.80  ISAKMP   Quick Mode

Frame 9210 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
```

```
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 292
  Encrypted payload (264 bytes)

No.     Time        Source        Destination   Protocol Info
9211    768.437057  10.20.129.80  10.20.131.62  ISAKMP   Quick Mode

Frame 9211 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 52
  Encrypted payload (24 bytes)
```

Data Security Regulations 16

Below are descriptions of each of the regulations available within NSX Data Security.

This chapter includes the following topics:

- "Arizona SB-1338," on page 221
- "ABA Routing Numbers," on page 221
- "Australia Bank Account Numbers," on page 221
- "Australia Business and Company Numbers," on page 221
- "Australia Medicare Card Numbers," on page 222
- "Australia Tax File Numbers," on page 222
- "California AB-1298," on page 222
- "California SB-1386," on page 223
- "Canada Social Insurance Numbers," on page 223
- "Canada Drivers License Numbers," on page 223
- "Colorado HB-1119," on page 224
- "Connecticut SB-650," on page 224
- "Credit Card Numbers," on page 224
- "Custom Account Numbers," on page 224
- "EU Debit Card Numbers," on page 225
- "FERPA (Family Educational Rights and Privacy Act)," on page 225
- "Florida HB-481," on page 225
- "France IBAN Numbers," on page 225
- "France National Identification Numbers Policy," on page 225
- "Georgia SB-230 Policy," on page 226
- "Germany BIC Numbers Policy," on page 226
- "Germany Driving License Numbers Policy," on page 226
- "Germany IBAN Numbers Policy," on page 226
- "Germany National Identification Numbers Policy," on page 226

- "Germany VAT Numbers Policy," on page 226
- "Hawaii SB-2290 Policy," on page 227
- "HIPAA (Healthcare Insurance Portability and Accountability Act) Policy," on page 227
- "Idaho SB-1374 Policy," on page 227
- "Illinois SB-1633," on page 228
- "Indiana HB-1101 Policy," on page 228
- "Italy Driving License Numbers Policy," on page 228
- "Italy IBAN Numbers Policy.," on page 228
- "Italy National Identification Numbers Policy," on page 228
- "Kansas SB-196 Policy," on page 229
- "Louisiana SB-205 Policy," on page 229
- "Maine LD-1671 Policy," on page 229
- "Massachusetts CMR-201," on page 230
- "Minnesota HF-2121," on page 230
- "Montana HB-732," on page 230
- "Netherlands Driving Licence Numbers," on page 230
- "Nevada SB-347," on page 231
- "New Hampshire HB-1660," on page 231
- "New Jersey A-4001," on page 231
- "New York AB-4254," on page 232
- "New Zealand Inland Revenue Department Numbers," on page 232
- "New Zealand Ministry of Health Numbers," on page 232
- "Ohio HB-104," on page 232
- "Oklahoma HB-2357," on page 233
- "Patient Identification Numbers," on page 233
- "Payment Card Industry Data Security Standard (PCI-DSS)," on page 233
- "Texas SB-122," on page 233
- "UK BIC Numbers," on page 234
- "UK Driving Licence Numbers," on page 234
- "UK IBAN Numbers," on page 234
- "UK National Health Service Numbers," on page 234
- "UK National Insurance Numbers (NINO)," on page 234
- "UK Passport Numbers," on page 234
- "US Drivers License Numbers," on page 235
- "US Social Security Numbers," on page 235
- "Utah SB-69," on page 235
- "Vermont SB-284," on page 235

- "Washington SB-6043," on page 236
- "Data Security Content Blades," on page 236

Arizona SB-1338

Arizona SB-1338 is a state data privacy law which protects personally identifiable information. Arizona SB-1338 was signed into law April 26, 2006 and became effective December 31, 2006. The law applies to any person or entity that conducts business in Arizona and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

ABA Routing Numbers

A routing transit number (RTN) or ABA number is a nine digit bank code, used in the United States, which appears on items such as checks that identifies which financial institution it is drawn upon. This code is also used by the Automated Clearing House to process direct deposits and other automated transfers. This system is named after the American Bankers Association, which designed it in 1910.

There are approximately 24,000 active routing and transit numbers currently in use. Every financial institution has one of these; it is a 9-digit number printed in MICR font at the bottom of checks that specifically identifies which financial institution it is associated with, and it is governed by the Routing Number Administrative Board which is sponsored by the ABA.

The primary purposes of the routing number are:

- To identify the bank which is responsible to either pay or give credit or is entitled to receive payment or credit for a financial transaction.
- To provide a reference to a designated presentment point of the bank at which the transaction can be delivered or presented.

For more information, see "ABA Routing Number Content Blade," on page 236.

Australia Bank Account Numbers

An Australian bank account number, along with a BSB (Bank-State-Branch number) identifies the bank account of an individual or organization.

Australia Business and Company Numbers

Australia Business Numbers (ABN) and Australia Company Numbers (ACN) uniquely identify businesses within the country.

The ABN is a unique 11-digit identifying number that businesses use when dealing with other businesses. A company's ABN frequently includes the ACN as the last nine digits. The ABN indicates that a person, trust or company is registered with the Australian Business Register (ABR).

An Australian Company Number (usually shortened to ACN) is a unique 9-digit number issued by the Australian Securities and Investments Commission (ASIC) to every company registered under the Commonwealth Corporations Act 2001 as an identifier. The number is usually printed in three groups of three digits.

Companies are required to disclose their ACN on:

- the common seal (if any)
- every public document issued, signed or published by, or on behalf of, the company
- every eligible negotiable instrument issued, signed or published by, or on behalf of, the company
- all documents required to be lodged with ASIC

This regulation uses the content blades titled Australia Business Number or Australia Company Number.

Australia Medicare Card Numbers

All Australian citizens and permanent residents of Australia and their families are eligible for a Medicare Card, with the exception of residents on Norfolk Island. The card lists an individual as well as members of his or her family he or she chooses to add who are also permanent residents and meet the Medicare definition of a dependent (maximum of five names). It is necessary to provide a Medicare Number for a Medicare rebate or to gain access to the public hospital system to be treated at no cost as a public patient.

Medicare is administered by Medicare Australia (known as the Health Insurance Commission until late 2005) which also has the responsibility for supplying Medicare cards and numbers. Almost every eligible person has a card: in June 2002 there were 20.4 million Medicare card-holders, and the Australian population was less than 20 million at the time (card-holders includes overseas Australians who still have a card).

The Medicare card is used for health care purposes only and cannot be used to track in a database. It contains a name and number, and no visible photograph (with the exception of the Tasmanian "Smartcard" version which does have an electronic image of the cardholder on an embedded chip).

The primary purpose of the Medicare card is to prove Medicare eligibility when seeking Medicare-subsidized care from a medical practitioner or hospital. Legally, the card need not be produced and a Medicare number is sufficient. In practice, most Medicare providers will have policies requiring the card be presented to prevent fraud.

Australia Tax File Numbers

A Tax File Number (TFN) is a number that is issued to a person by the Commissioner of Taxation and is used to verify client identity and establish income level.

This policy uses the content blade titled Australia Tax File Number. Refer to the description of the content blades to understand what content will be detected.

California AB-1298

California AB-1298 is a state data privacy law which protects personally identifiable information. California AB-1298 in was signed into law October 14, 2007 and became effective January 1, 2008. The law applies to any person, business, or state agency that conducts business in California and owns or licenses unencrypted computerized data that includes personally identifiable information.

This law is an amendment to California SB-1386 to include medical information and health information in the definition of personal information.

The regulation looks for at least one match to personally identifiable information, as defined through the following content blades:

- Admittance and Discharge Dates
- Credit Card Numbers
- Credit Card Track Data

- Group Insurance Numbers
- Health Plan Beneficiary Numbers
- Healthcare Dictionaries
- Medical History
- Patient Identification Numbers
- US Drivers License Numbers
- US National Provider Identifiers
- US Social Security Numbers

California SB-1386

California SB-1386 is a state data privacy law which protects personally identifiable information. California SB-1386 was signed into law September 25, 2002 and became effective July 1, 2003. The law applies to any person, business, or state agency that conducts business in California and owns or licenses unencrypted computerized data that includes personally identifiable information.

This law has been amended to include medical information and health information; it is now referred to as California AB-1298, which is provided as an expanded regulation in the SDK. If California AB-1298 is enabled, you do not need to also use this regulation as the same information is detected as part of AB-1298.

The regulation looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Canada Social Insurance Numbers

A Social Insurance Number (SIN) is a number issued in Canada to administer various government programs. The SIN was created in 1964 to serve as a client account number in the administration of the Canada Pension Plan and Canada's varied employment insurance programs. In 1967, Revenue Canada (now the Canada Revenue Agency) started using the SIN for tax reporting purposes.

Canada Drivers License Numbers

In Canada, driver's licenses are issued by the government of the province in which the driver resides. Thus, specific regulations relating to driver's licenses vary province to province, though overall they are quite similar. All provinces have provisions allowing non-residents to use licenses issued by other provinces and International Driving Permits.

The regulation looks for at least a match to at least one of the following content blades:

- Alberta Drivers Licence
- British Columbia Drivers Licence
- Manitoba Drivers Licence
- New Brunswick Drivers Licence
- Newfoundland and Labrador Drivers Licence
- Nova Scotia Drivers Licence

  License pattern rules: 5 letters followed by 9 digits

- Ontario Drivers Licence
- Prince Edward Island Drivers Licence
- Quebec Drivers Licence
- Saskatchewan Drivers Licence

Colorado HB-1119

Colorado HB-1119 is a state data privacy law which protects personally identifiable information. Colorado HB-1119 was signed into law April 24, 2006 and became effective September 1, 2006. The law applies to any individual or a commercial entity that conducts business in Colorado and owns or licenses unencrypted computerized data that includes personally identifiable information.

The regulation looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Connecticut SB-650

Connecticut SB-650 is a state data privacy law which protects personally identifiable information. Connecticut SB-650 was signed into law June 8, 2005 and became effective January 1, 2006. The law applies to any person, business or agency that conducts business in Connecticut and owns or licenses unencrypted computerized data that includes personally identifiable information.

The regulation looks for at least one match to personally identifiable information, as defined through the following content blades:

- Admittance and Discharge Dates
- Birth and Death Certificates
- Credit Card Numbers
- Credit Card Track Data
- Group Insurance Numbers
- Health Plan Beneficiary Numbers
- Healthcare Dictionaries
- Medical History
- Patient Identification Numbers
- US Drivers License Numbers
- US National Provider Identifiers
- US Social Security Numbers

Credit Card Numbers

Custom Account Numbers

If you have organizational account numbers that need to be protected, then customize the content blade assigned to the Custom Account Numbers regulation with the number pattern via a regular expression.

EU Debit Card Numbers

The policy looks for debit card numbers as issued by the major debit card carriers in the European Union such as Maestro, Visa and Laser.

FERPA (Family Educational Rights and Privacy Act)

FERPA protects the privacy of student records at educational institutions receiving U.S. Department of Education funds. It requires the educational institution to have written permission from a parent or student in order to release information from a student's educational record.

Under certain circumstances the release of information such as name, address, telephone number, honors and awards, and dates of attendance may be released or published without permission. Information that can connect an individual with grades or disciplinary actions requires permission.

The policy must match both of the following content blades for a document to trigger as a violation:

- Student Identification Numbers
- Student Records

Florida HB-481

Florida HB-481 is a state data privacy law which protects personally identifiable information. Florida HB-481 was signed into law June 14, 2005 and became effective July 1, 2005. The law applies to any person, firm, association, joint venture, partnership, syndicate, corporation, and all other groups or combinations that conduct business in Florida and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

France IBAN Numbers

A France International Bank Account Number (IBAN) is an international standard for identifying France bank accounts across national borders and was originally adopted by the European Committee for Banking Standards. The official IBAN registrar under ISO 13616:2003 is issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

The policy looks for a match to the content blade France IBAN Number.

France National Identification Numbers Policy

The policy identifies documents and transmissions that contain national identification numbers, also called INSEE numbers and Social Security numbers, issued to individuals at birth by the Institut National de la Statistique et des Etudes Economiques (INSEE) in France.

The policy looks for a match to the content blade France National Identification Number.

Georgia SB-230 Policy

Georgia SB-230 is a state data privacy law which protects personally identifiable information. Georgia SB-230 was signed into law May 5, 2005 and became effective May 5, 2005. The law applies to any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personally identifiable information to nonaffiliated third parties, or any state or local agency or subdivision thereof that maintains data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Germany BIC Numbers Policy

A Bank Identifier Code (BIC) uniquely identifies a particular bank and is used in Germany and worldwide for the exchange of money and messages between banks. The policy identifies documents and transmissions that contain BIC codes, also known as SWIFT codes, issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

The policy looks for a match to the content blade Germany BIC Number.

Germany Driving License Numbers Policy

A Germany Drivers License Number is an identification number on a German Drivers License and identifies the owner of said number for the purposes of driving and driving offences.

The policy looks for a match to the content blade Germany Driving License Number.

Germany IBAN Numbers Policy

International Bank Account Number (IBAN) is an international standard for identifying bank accounts across national borders and was originally adopted by the European Committee for Banking Standards. The official IBAN registrar under ISO 13616:2003 is issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

The policy looks for a match to the content blade Germany IBAN Number.

Germany National Identification Numbers Policy

The policy identifies documents and transmissions that contain personal identification numbers, or Personalausweis, issued to individuals in Germany.

The policy looks for a match to the content blade Germany National Identification Number.

Germany VAT Numbers Policy

based business or legal entity for the purposes of levying Value Added Tax (or goods and services tax).

The policy looks for a match to the content blade Germany VAT Number.

Hawaii SB-2290 Policy

Hawaii SB-2290 is a state data privacy law which protects personally identifiable information.

Hawaii SB-2290 was signed into law May 25, 2006 and became effective January 1, 2007. The law applies to any sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit, including financial institutions organized, chartered, or holding a license or authorization certificate under the laws of Hawaii, any other state, the US, or any other country, or the parent or the subsidiary of any such financial institution, and any entity whose business is records destruction, or any government agency that collects personally identifiable information for specific government purposes

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

HIPAA (Healthcare Insurance Portability and Accountability Act) Policy

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the Congress of the United States of America. HIPAA includes a Privacy Rule regulating the use and disclosure of protected health information (PHI), a Security Rule defining security safeguards required for electronic protected health information (ePHI), and an Enforcement Rule that defines procedures for violation investigations and penalties for confirmed violations.

PHI is defined as individually identifiable health information that is transmitted or maintained in any form or medium (electronic, oral, or paper) by a covered entity or its business associates, excluding certain educational and employment records. Individually identifiable means the identity of the subject is or may readily be ascertained by the investigator or associated with the information.

This policy is designed to detect electronic PHI, which contains a personal health number in addition to health-related terminology. Some false negatives may occur since combinations of personally identifiable information, such as name and address, would not be considered as ePHI with this policy. Internal research indicates that the majority of health communication will contain a personal health number in addition to health-related terminology.

Idaho SB-1374 Policy

Idaho SB-1374 is a state data privacy law which protects personally identifiable information. Idaho SB-1374 was signed into law March 30, 2006 and became effective July 1, 2006. The law applies to any agency, individual, or commercial entity that conducts business in Idaho and owns or licenses unencrypted computerized data that includes personally identifiable information about a resident of Idaho.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Illinois SB-1633

Illinois SB-1633 is a state data privacy law which protects personally identifiable information. Illinois SB-1633 was signed into law June 16, 2005 and became effective June 27, 2006.

The law applies to any data collector, which includes, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personally identifiable information that owns or licenses personally identifiable information concerning an Illinois resident.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Indiana HB-1101 Policy

Indiana HB-1101 is a state data privacy law which protects personally identifiable information. Indiana HB-1101 was signed into law April 26, 2005 and became effective July 1, 2006. The law applies to any individual, corporation, business trust, estate, trust partnership, association, nonprofit corporation or organization, cooperative, or any other legal entity that owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Italy Driving License Numbers Policy

A Italy Drivers License Number is an identification number on a Italian Drivers License and identifies the owner of said number for the purposes of driving and driving offences.

The policy looks for a match to the content blade Italy Driving License Number.

Italy IBAN Numbers Policy.

A International Bank Account Number (IBAN) is an international standard for identifying bank accounts across national borders and was originally adopted by the European Committee for Banking Standards. The official IBAN registrar under ISO 13616:2003 issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)

The policy looks for a match to the content blade Italy IBAN Number.

Italy National Identification Numbers Policy

The policy identifies documents and transmissions that contain personal identification numbers, or Codice Fiscale, issued to individuals in Italy.

The policy looks for a match to the content blade Italy National Identification Number.

Kansas SB-196 Policy

Kansas SB-196 is a state data privacy law which protects personally identifiable information. Kansas SB-196 was signed into law April 19, 2006 and became effective January 1, 2007. The law applies to any individual, partnership, corporation, trust, estate, cooperative, association, government, or government subdivision or agency or other entity that conducts business in Kansas and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Louisiana SB-205 Policy

Louisiana SB-205 is a state data privacy law which protects personally identifiable information. Louisiana SB-205 was signed into law July 12, 2005 and became effective January 1, 2006. The law applies to any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity that conducts business in Louisiana and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Maine LD-1671 Policy

Maine LD-1671 is a state data privacy law which protects personally identifiable information. Maine LD-1671 was signed into law June 10, 2005 and became effective January 31, 2006.

The law applies to any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association, or other entity, including agencies of state government, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private collages and universities, or any information in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personally identifiable information to nonaffiliated third parties that maintains computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Massachusetts CMR-201

Massachusetts CMR-201 is a state data privacy regulation which protects personally identifiable information. Massachusetts CMR-201 was issued on September 19, 2008 and became effective May 1, 2009. The regulation applies to all businesses and other legal entities that own, license, collect, store or maintain personal information about a resident of the Commonwealth of Massachusetts.

The policy looks for at least one match to personally identifiable information, which may include:

- ABA Routing Numbers
- Credit Card Number
- Credit Card Track Data
- US Bank Account Numbers
- US Drivers License Number
- US Social Security Number

Minnesota HF-2121

Minnesota HF-2121 is a state data privacy law which protects personally identifiable information. Minnesota HF-2121 was signed into law June 2, 2005 and became effective January 1, 2006. The law applies to any person or business that conducts business in Minnesota and owns or licenses data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Montana HB-732

Montana HB-732 is a state data privacy law which protects personally identifiable information. Montana HB-732 was signed into law April 28, 2005 and became effective March 1, 2006. The law applies to any person or business that conducts business in Montana and owns or licenses computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Netherlands Driving Licence Numbers

A Netherlands Driving License number is an identification number on a Netherlands Drivers License and identifies the owner of said number for the purposes of driving and driving offences.

The policy looks for a match to the content blade Netherlands Driving License Number.

Nevada SB-347

Nevada SB-347 is a state data privacy law which protects personally identifiable information. Nevada SB-347 was signed into law June 17, 2005 and became effective October 1, 2005. The law applies to any government agency, institution of higher education, corporation, financial institution or retail operator, or any other type of business entity or association that owns computerized data which includes personal information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

New Hampshire HB-1660

New Hampshire HB-1660 is a state data privacy law which protects personally identifiable information. New Hampshire HB-1660 was signed into law June 2, 2006 and became effective January 1, 2007. The law applies to any individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state doing business in New Hampshire that owns or licenses computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

New Jersey A-4001

New Jersey A-4001 is a state data privacy law which protects personally identifiable information.

New Jersey A-4001 was signed into law September 22, 2005 and became effective January 1, 2006. The law applies to New Jersey, and any country, municipality, district, public authority, public agency, and any other political subdivision or public body in New Jersey, any sole proprietorship, partnership, corporation, association, or other entity, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of New Jersey, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution, that conducts business in New Jersey that compiles or maintains computerized records that include personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

New York AB-4254

New York AB-4254 is a state data privacy law which protects personally identifiable information. New York AB-4254 was signed into law August 10, 2005 and became effective December 8, 2005. The law applies to any person or business which conducts business in New York and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

New Zealand Inland Revenue Department Numbers

The policy identifies documents and transmissions that contain New Zealand Inland Revenue Department (IRD) numbers issued by the Inland Revenue Department to every taxpayer and organization. The number must be provided by an individual to the Inland Revenue, employers, banks or other financial institutions, KiwiSaver scheme providers, StudyLink and tax agents.

The policy looks for a match to the content blade New Zealand Inland Revenue Department Number.

New Zealand Ministry of Health Numbers

The policy identifies documents and transmissions that contain New Zealand Health Practitioner Index (HPI) or National Health Index (NHI) numbers.

The New Zealand Ministry of Health, or Manatū Hauora in Māori, is the New Zealand government's principal agent and advisor on health and disability. The agency uses the NHI numbering system for registering patients and the HPI system for registering medical practitioners to ensure that records are accurate while protecting the privacy of individuals. This policy detects 6-digit alphanumeric New Zealand Health Practitioner Index Common Person numbers (HPI-CPN), which uniquely identify a health practitioner or worker. This policy also detects 7-digit NHI numbers used to uniquely identify a patient within the New Zealand health system.

The policy looks for a match to either of the content blades:

- New Zealand Health Practitioner Index Number
- New Zealand National Health Index Number

Ohio HB-104

Ohio HB-104 is a state data privacy law which protects personally identifiable information. Ohio HB-104 was signed into law November 17, 2005 and became effective December 29, 2006. The law applies to any individual, corporation, business trust, estate, trust, partnership, or association that conducts business in Ohio and owns or licenses computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Oklahoma HB-2357

Oklahoma HB-2357 is a state data privacy law which protects personally identifiable information. Oklahoma HB-2357 was signed into law June 8, 2006 and became effective November 1, 2008. The law applies to any corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit that conducts business in Oklahoma HB-2357 and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Patient Identification Numbers

The personally identifiable information (PII) commonly held by hospitals and healthcare-related organizations and businesses in the United States of America. This policy should be customized to define the patient identification number format.

The policy looks for at least one match to personally identifiable information, which may include:

- Patient Identification Numbers
- US National Provider Identifier
- US Social Security Number

Payment Card Industry Data Security Standard (PCI-DSS)

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The policy looks for at least one match to either of the content blades:

- Credit Card Number
- Credit Card Track Data

Texas SB-122

Texas SB-122 is a state data privacy law which protects personally identifiable information. Texas SB-122 was signed into law June 17, 2005 and became effective September 1, 2005. The law applies to any person that conducts business in Texas and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number

- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

UK BIC Numbers

A Bank Identifier Code (BIC) uniquely identifies a particular bank and is used in the UK and worldwide for the exchange of money and messages between banks. The policy identifies documents and transmissions that contain BIC codes, also known as SWIFT codes, issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

The policy looks for a match to the content blade UK BIC Number.

UK Driving Licence Numbers

A UK driving license number is an identification number on a UK driving license and identifies the owner of said number for the purposes of driving and driving offences.

The policy looks for a match to the content blade UK Driving License Number.

UK IBAN Numbers

International Bank Account Number (IBAN) is an international standard for identifying the UK bank accounts across national borders and was originally adopted by the European Committee for Banking Standards. The official IBAN registrar under ISO 13616:2003 is issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

The policy looks for a match to the content blade UK IBAN Number.

UK National Health Service Numbers

A UK National Health Service number is an identification number provided by the UK National Health Service and identifies the owner of said number for the purposes of medical records.

The policy looks for a match to the content blade UK National Health Service Number.

UK National Insurance Numbers (NINO)

UK National Insurance is a system of payments made out of earnings by employees, employers and the self-employed to the Government that entitle you to a state pension and other benefits.

UK National Insurance Numbers (NINO) are the identification numbers assigned to each person born in the UK, or to anyone resident in the UK who is a legal employee, student, recipient of social welfare benefits, pension etc.

The policy looks for a match at least one of the content blades UK NINO Formal or UK NINO Informal.

UK Passport Numbers

The policy identifies documents and transmissions that contain passport numbers issued in the UK.

The policy looks for a match to the content blade UK Passport Number.

US Drivers License Numbers

Driver's licenses issued in the United States have a number or alphanumeric code issued by the Department of Motor Vehicles (or equivalent), usually show a photograph of the bearer, as well as a copy of his or her signature, the address of his or her primary residence, the type or class of license, restrictions and/or endorsements (if any), the physical characteristics of the bearer (such as height, weight, hair color, eye color, and sometimes even skin color), and birth date. No two driver's license numbers issued by a state are alike. Social Security numbers are becoming less common on driver's licenses, due to identity theft concerns.

The policy looks for a match to the content blade US Drivers Licenses.

US Social Security Numbers

The U.S. Social Security number is issued to U.S. citizens, permanent residents, and temporary (working) residents under section 205(c)(2) of the Social Security Act, codified as 42 U.S.C. § 405(c)(2). The number is issued to an individual by the Social Security Administration, an independent agency of the United States government. Its primary purpose is to track individuals for taxation purposes.

Utah SB-69

Utah SB-69 is a state data privacy law which protects personally identifiable information. Utah SB-69 was signed into law March 20, 2006 and became effective January 1, 2007. The law applies to any who owns or license computerized data that includes personally identifiable information concerning a Utah resident.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Vermont SB-284

Vermont SB-284 is a state data privacy law which protects personally identifiable information. Vermont SB-284 was signed into law May 18, 2006 and became effective January 1, 2007. The law applies to any data collector that owns or licenses unencrypted computerized data that includes personally identifiable information concerning an individual residing in Vermont.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Washington SB-6043

Washington SB-6043 is a state data privacy law which protects personally identifiable information. Washington SB-6043 was signed into law May 10, 2005 and became effective July 24, 2005. The law applies to any state or local agency or any person or business which conducts business in Washington and owns or licenses computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Data Security Content Blades

This sections lists the available content blades for NSX regulations.

ABA Routing Number Content Blade

The content blade looks for matches to 3 pieces of information in close proximity of each other.

The content blade looks for:

- ABA routing number
- Banking words and phrases (e.g. aba, routing number, checking, savings)
- Personally identifiable information (e.g. name, address, phone number)

Words and phrases related to banking are implemented in order to increase precision. A routing number is 9-digits and may pass for many different data types, for example, a valid US Social Security number, Canadian Social Insurance number or international telephone number.

Since routing numbers themselves are not sensitive, personally identifiable information is necessary for a violation to occur.

Admittance and Discharge Dates Content Blade

The content blade looks for matches to the U. S. Date Format entity and words and phrases such as admit date, admittance date, date of discharge, discharge date in close proximity to each other.

Alabama Drivers License Content Blade

The content blade looks for matches to the Alabama driver's license pattern and words and phrases such as driver's license and license number and, optionally, terms such as AL or Alabama.

Driver's license pattern

7 Numeric or 8 Numeric

Alaska Drivers License Content Blade

The content blade looks for matches to the Alaska driver's license pattern and words and phrases such as driver's license and license number and, optionally, terms such as AK or Alaska.

Driver's license pattern:

7 Numeric

Alberta Drivers Licence Content Blade

The content blade looks for matches to the Alberta driver’s license pattern and words and phrases such as driver’s license and license number and, optionally, terms such as AK or Alberta.

Driver's license pattern

7 Numeric

Alaska Drivers License Content Blade

The content blade looks for matches to the Alaska driver’s license pattern and words and phrases such as driver’s license and license number and, optionally, terms such as AK or Alaska.

Driver's license pattern:

7 Numeric

Alberta Drivers Licence Content Blade

The content blade looks for matches to the Alberta driver’s license pattern and words and phrases such as driver’s license and license number and, optionally, terms such as AK or Alberta.

Driver's license pattern

7 Numeric

American Express Content Blade

The content blade looks for a combination of the following pieces of information.

- More than one American Express credit card number
- A single credit card number plus words and phrases such as ccn, credit card, expiration date
- A single credit card number plus an expiration date

Arizona Drivers License Content Blade

The content blade looks for matches to the Arizona driver’s license pattern and words and phrases such as driver’s license and license number and, optionally, terms such as AZ or Arizona.

The Driver's license pattern can be 1 Alphabetic, 8 Numeric; or 9 Numeric (SSN); or 9 Numeric (Unformatted SSN).

Arkansas Drivers License Content Blade

The content blade looks for matches to the Arkansas driver’s license pattern and words and phrases such as driver’s license and license number and, optionally, terms such as AR or Arkansas.

Driver's license pattern can be 9, 8 Numeric.

Australia Bank Account Number Content Blade

The Australian bank account number itself is not sensitive, but identifies a bank account, without identifying the bank branch. Therefore, both the account number and branch information must exist for the document to be considered sensitive.

The content blade looks for matches to both:

- An Australian bank account number
- Words and phrases related to bank state branch or BSB.

It also uses a regular expression rule to differentiate between telephone numbers of the same length.

An Australian bank account number is 6 to 10-digits without any embedded meaning. It has no check digit routine.

Australia Business Number Content Blade

The content blade looks for matches to both pieces of information in close proximity to each other.

- Australia Business Number
- ABN words and phrases (e.g. ABN, Australia business number)

Australia Company Number Content Blade

The content blade looks for matches to both pieces of information in close proximity to each other.

- Australia Company Number
- ACN words and phrases (e.g. ACN, Australia Company Number)

Australia Medicare Card Number Content Blade

The content blade will match if one of the following combinations of information appears in a document.

- More than one Australia Medicare Card Number
- One Medicare card number plus Medicare or patient identification terms (e.g. patient identifier, patient number)
- One Medicare card number plus two of either a name, expiration date or expiration terms

Australia Tax File Number Content Blade

The content blade looks for matches to both pieces of information in high proximity to each other.

- Australia Tax File Number (refer to entity description)
- Tax file number words and phrases (e.g. TFN, tax file number)

California Drivers License Number Content Blade

The content blade looks for matches to the California driver’s license pattern and words and phrases such as driver’s license and license number and terms such as CA or California.

The Driver's license pattern is 1 Alphabetic, 7 Numeric.

Canada Drivers License Number Content Blade

The content blade is only a container file for child content blades. The content blades assigned to it separately look for driver's licenses in individual providences and territories.

Canada Social Insurance Number Content Blade

The content blade is only a container file for child content blades. The content blades assigned to it separately look for formatted and unformatted versions of the Canadian Social Insurance numbers plus personal information so different rules may be assigned to them. The formatted version of the Social Insurance number is a more specific pattern, so the rules are less strict for retuning a match. However, the unformatted version is very general and matches to many common numbers.

Colorado Drivers License Number Content Blade

The content blade looks for matches to the Colorado driver’s license pattern and words and phrases such as driver’s license and license number and terms such as CO or Colorado.

The driver's license pattern is 9 Numeric.

Connecticut Drivers License Number Content Blade

The content blade looks for matches to the Connecticut driver’s license pattern and words and phrases such as driver’s license and license number and terms such as CT or Connecticut.

Driver's license pattern: 9 Numeric, 1st two positions are month of birth in odd or even year. 01-12 Jan-Dec odd years, 13-24 Jan-Dec even years, 99 unknown.

Credit Card Number Content Blade

The content blade looks for a combination of the following pieces of information.

- More than one credit card number
- A single credit card number plus words and phrases such as ccn, credit card, expiration date
- A single credit card number plus an expiration date

Credit Card Track Data Content Blade

Track data is the information encoded and stored on two tracks located within the magnetic stripe on the back of a credit card (debit card, gift card, etc). There are three tracks on the magstripe (magnetic strip on the back of a credit card).

Each track is .110-inch wide. The ISO/IEC standard 7811, which is used by banks, specifies:

- Track one is 210 bits per inch (bpi), and holds 79 six-bit plus parity bit read-only characters.
- Track two is 75 bpi, and holds 40 four-bit plus parity bit characters.
- Track three is 210 bpi, and holds 107 four-bit plus parity bit characters.

Your credit card typically uses only tracks one and two. Track three is a read/write track (that includes an encrypted PIN, country code, currency units, amount authorized), but its usage is not standardized among banks.

This content blade requires a match to the Credit Card Track Data entity.

Custom Account Number Content Blade

The Custom Accounts content blade is an editable blade and should contain a regular expression for an organization's custom account patterns.

Delaware Drivers License Number Content Blade

The content blade looks for matches to the Delaware driver's license pattern and words and phrases such as driver's license and license number and terms such as DE or Delaware.

EU Debit Card Number Content Blade

The content blade looks for patterns of the major European Union debit card numbers.

The content blade will match with a combination of the following pieces of information in close proximity, if either:

- More than one match to a EU debit card number
- A single match to a EU debit card number plus two of either a word or phrase for credit card (e.g. card number or cc#), credit card security, expiration date or name
- A single match to a EU debit card number with an expiration date

Florida Drivers License Number Content Blade

The content blade looks for matches to the Florida driver's license pattern and words and phrases such as driver's license and license number and terms such as FL or Florida.

Driver's license pattern: 1 Alphabetic, 12 Numeric.

France Driving License Number Content Blade

The content blade requires the following to match for a French driving license in a close proximity.

- French driving license pattern
- Either words or phrases for a driving license (e.g. driving license, permis de conduire) or E.U. date format

France BIC Number Content Blade

The content blade scans for French BIC numbers by requiring matches for both the following rules.

- European BIC number format
- French format of the BIC number

France IBAN Number Content Blade

The content blade requires the following to match for a French IBAN number in a close proximity.

- European IBAN number format
- French IBAN number pattern

France National Identification Number Content Blade

The content blade requires the following to match for a French National Identification number in a close proximity.

- More than one match to the French National Identification pattern
- One match to the French National Identification pattern plus either words or phrases for a social security number (e

France VAT Number Content Blade

The content blade requires a match for a French value added tax (VAT) number pattern in a close proximity to the abbreviation FR.

Georgia Drivers License Number Content Blade

The content blade looks for matches to the Georgia driver's license pattern and words and phrases such as driver's license and license number and terms such as GA or Georgia.

Driver's license pattern: 7-9 Numeric; or Formatted SSN.

Germany BIC Number Content Blade

The content blade scans for German BIC numbers by requiring matches for both the following rules.

- European BIC number format
- German format of the BIC number

Germany Driving License Number Content Blade

The content blade requires the following to match for a German driving license in a close proximity.

- German driving license pattern
- Words or phrases related to a driving license (e.g. driving license, ausstellungsdatum)

Germany IBAN Number Content Blade

The content blade requires the following to match for a German IBAN number in a close proximity.

- European IBAN number format
- German IBAN number pattern

THe German IBAN rule: "DE" country code followed by 22 digits.

Germany National Identification Numbers Content Blade

The content blade requires the following to match for a German National Identification number in a close proximity.

- Either a German National Identification number or a machine-readable version of the number
- Words or phrases for a German National Identification number (e.g. personalausweis, personalausweisnummer)

Germany Passport Number Content Blade

The content blade requires the following to match for a German passport number in a close proximity.

- Either a German passport number or a machine-readable version of the number
- Words or phrases for a German passport number or issuance date (e.g. reisepass, ausstellungsdatum)

Germany VAT Number Content Blade

The content blade requires a match for a German value added tax (VAT) number pattern (refer to entity description) in a close proximity to the abbreviation DE.

Group Insurance Numbers Content Blade

This is a content blade that requires customization. To use this content blade, add a regular expression to match the number pattern for an organization's Group Insurance Number. The content blade looks for matches to words and phrases such as group insurance or a name, U.S. address or U.S. date in combination with the custom regular expression.

Hawaii Drivers License Number Content Blade

The content blade looks for matches to the Hawaii driver's license pattern and words and phrases such as driver's license and license number and terms such as HI or Hawaii.

Driver's license pattern: H Alphabetic, 8 Numeric; or SSN.

Italy National Identification Numbers Content Blade

The content blade requires the following to match for an Italy National Identification number in a close proximity.

1 Italy National Identification number pattern

2 Words or phrases for an Italy National Identification number (e.g. codice fiscale, national identification)

National Identification Rule: 16 character alphanumeric code. where:

- *SSS* are the first three consonants in the family name (the first vowel and then an X are used if there are not enough consonants)
- *NNN* is the first name, of which the first, third and fourth consonants are used—exceptions are handled as in family names
- *YY* are the last digits of the birth year
- *M* is the letter for the month of birth—letters are used in alphabetical order, but only the letters A to E, H, L, M, P, R to T are used (thus, January is A and October is R)
- *DD* is the day of the month of birth—in order to differentiate between genders, 40 is added to the day of birth for women (thus a woman born on May 3 has ...E43...)
- *ZZZZ* is an area code specific to the municipality where the person was born—country-wide codes are used for foreign countries, a letter followed by three digits

- *X* is a parity character as calculated by adding together characters in the even and odd positions, and dividing them by 26. Numerical values are used for letters in even positions according to their alphabetical order. Characters in odd positions have different values. A letter is then used which corresponds to the value of the remainder of the division in the alphabet.

Pattern:

- *LLLLLLDDLDDLDDDL*
- *LLL LLL DDLDD LDDDL*

Health Plan Beneficiary Numbers

This is a content blade that requires customization. To use this content blade, add a regular expression to identify recipients of health plan benefits and payments. The content blade looks for matches to words and phrases such as beneficiary or a name, U.S. address or U.S. date in combination with the custom regular expression.

Idaho Drivers License Number Content Blade

The content blade looks for matches to the Idaho driver's license pattern and words and phrases such as driver's license and license number and terms such as ID or Idaho.

Driver's license pattern: 2 Alphabetic, 6 Numeric, 1 Alphabetic.

Illinois Drivers License Number Content Blade

The content blade looks for matches to the Illinois driver's license pattern and words and phrases such as driver's license and license number and terms such as IL or Illinois.

Driver's license pattern: 1 Alphabetic, 11 Numeric.

Indiana Drivers License Number Content Blade

The content blade looks for matches to the Indiana driver's license pattern and words and phrases such as driver's license and license number and terms such as IN or Indiana.

Driver's license pattern: 10 Numeric.

Iowa Drivers License Number Content Blade

The content blade looks for matches to the Iowa driver's license pattern and words and phrases such as driver's license and license number and terms such as IA or Iowa.

Driver's license pattern can be 3 numeric, 2 alphabetic, 3 numeric; or Social Security Number.

Index of Procedures Content Blade

The content blade looks for words and phrases related to medical procedures based on the International Classification of Diseases (ICD).

The content blade will match with a combination of the following pieces of information, either:

- More than one match to the Index of Procedures dictionary
- A single match to the Index of Procedures dictionary plus two of either a name, U.S. Address or U.S. Date
- A single match to the Index of Procedures dictionary with a patient or doctor identification word or phrase (e.g. patient ID, physician name)

Italy Driving License Number Content Blade

The content blade requires the following to match for an Italy driving license in a close proximity.

- Italy driving license pattern
- Words or phrases for a driving license (e.g. driving license, patente di guida)

Driver's License Rule: 10 alphanumeric characters -- 2 letters, 7 numbers and a final letter. The first letter may only be characters A-V.

Driver's License Pattern:

- *LLDDDDDDDL*
- *LL DDDDDDD* L
- *LL-DDDDDDD-L*
- *LL - DDDDDDD - L*

Italy IBAN Number Content Blade

The content blade requires the following to match for a Italy IBAN number in a close proximity.

1 IBAN words and phrases (e.g. International Bank Account Number, IBAN)

2 Italy IBAN number pattern

IBAN Rule: `IT` country code followed by 25 alphanumeric characters.

Pattern:

- `IT`*DDLDDDDDDDDDDAAAAAAAAAAAA*
- `IT` *DDL DDDDD DDDDD AAAAAAAAAAAA*
- `IT` *DD LDDDDD DDDDD AAAAAAAAAAAA*
- `IT` *DD L DDDDD DDDDD AAAAAAAAAAAA*
- `IT` *DD LDDDDDDDDDDAAAAAAAAAAAA*
- `IT` *DD L DDDDDDDDDDAAAAAAAAAAAA*
- `IT`*DD LDDD DDDD DDDA AAAA AAAA AAA*
- `IT` *DDL DDDDD DDDDD AAAAAA AAAAAA*
- `IT` *DDL DDD DDD DDD DAAA AAA AAAAAA*
- `IT` *DDL DDDDDDDDDD AAAAAA AAAAAA*

Spaces may be substituted with dashes, forward slashes or colons.

ITIN Unformatted Content Blade

The content blade looks for unformatted patterns of the U.S. Taxpayer Identification Number (ITIN). The content blade will match if an unformatted ITIN is found within close proximity of a word or phrase for an ITIN number (e.g. tax identification, ITIN).

ITIN Rule: 9-digit number that always begins with the number 9 and has a range of 70-88 in the fourth and fifth digit.

Pattern: *DDDDDDDDD*

Kansas Drivers License Number Content Blade

The content blade looks for matches to the Kansas driver's license pattern and words and phrases such as driver's license and license number and terms such as KS or Kansas.

Driver's license pattern: 1 Alphabetic (K), 8 Numeric; or Social Security Number.

Kentucky Drivers License Number Content Blade

The content blade looks for matches to the Kentucky driver's license pattern and words and phrases such as driver's license and license number and terms such as KY or Kentucky.

Driver's license pattern: 1 Alphabetic, 8 Numeric; or Social Security Number.

Louisiana Drivers License Number Content Blade

The content blade looks for matches to the Louisiana driver's license pattern and words and phrases such as driver's license and license number and terms such as LA or Louisiana.

Driver's license pattern: 2 Zeros, 7 Numeric.

Maine Drivers License Number Content Blade

The content blade looks for matches to the Maine driver's license pattern and words and phrases such as driver's license and license number and terms such as ME or Maine.

Driver's license pattern: 7 Numeric, optional alphabetic X.

Manitoba Drivers Licence Content Blade

The content blade looks for matches to the Manitoba driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as MB or Manitoba in a close proximity.

License pattern rules: 12 alphanumeric characters that may be hyphen-separated, where:

- 1st character is a letter
- 2nd - 5th characters are a letter or asterisk
- 6th character is a letter
- 7th - 10th characters are digits
- 11th character is a letter
- 12th character is a letter or digit

or

- 1st character is a letter
- 2nd - 4th characters are a letter or asterisk
- 5th - 6th characters are digits
- 7th - 12th characters are a letter or digit

Driver's license pattern:

- *LLLLLLDDDDLA*
- *LLLLLDDAAAAAA*

Maryland Drivers License Number Content Blade

The content blade looks for matches to the Maryland driver's license pattern and words and phrases such as driver's license and license number and terms such as MD or Maryland.

Driver's license pattern: 1 Alphabetic, 12 Numeric

Massachusetts Drivers License Number Content Blade

The content blade looks for matches to the Massachusetts driver's license pattern and words and phrases such as driver's license and license number and terms such as MA or Massachusetts.

Driver's license pattern: 1 Alphabetic (S), 8 Numeric; or Social Security Number

Michigan Drivers License Number Content Blade

The content blade looks for matches to the Michigan driver's license pattern and words and phrases such as driver's license and license number and terms such as MI or Michigan.

Driver's license pattern: 1 Alphabetic, 12 Numeric

Minnesota Drivers License Number Content Blade

The content blade looks for matches to the Minnesota driver's license pattern and words and phrases such as driver's license and license number and terms such as MN or Minnesota.

Driver's license pattern: 1 Alphabetic, 12 Numeric

Mississippi Drivers License Number Content Blade

The content blade looks for matches to the Mississippi driver's license pattern and words and phrases such as driver's license and license number and terms such as MS or Mississippi.

Driver's license pattern: 9 Numeric; or Formatted Social Security Number

Missouri Drivers License Number Content Blade

The content blade looks for matches to the Missouri driver's license pattern and words and phrases such as driver's license and license number and terms such as MO or Missouri

Driver's license pattern: 1 Alphabetic, 6-9 Numeric; or 9 Numeric; or Formatted Social Security Number

Montana Drivers License Number Content Blade

The content blade looks for matches to the Montana driver's license pattern and words and phrases such as driver's license and license number and terms such as MT or Montana.

Driver's license pattern: 9 Numeric (SSN); or 1 Alphabetic, 1 Numeric, 1 Alphanumeric, 2 Numeric, 3 Alphabetic and 1 Numeric; or 13 Numeric

NDC Formulas Dictionary Content Blade

The content blade looks for words and phrases related to formulas based on the National Drug Codes (NDC).

The content blade will match with a combination of the following pieces of information, either:

1 More than one match to the NDC Formulas dictionary

2 A single match to the NDC Formulas dictionary plus two of either a name, U.S. Address or U.S. Date

3 A single match to the NDC Formulas dictionary with a patient or doctor identification word or phrase (e.g. patient ID, physician name)

Nebraska Drivers License Number Content Blade

The content blade looks for matches to the Nebraska driver's license pattern and words and phrases such as driver's license and license number and terms such as NE or Nebraska.

Driver's license pattern: 1 Alphabetic , 8 Numeric

Netherlands Driving Licence Number Content Blade

The content blade requires the following to match for a Netherlands driving license in a close proximity.

1 Netherlands driving license pattern (refer to entity description)

2 Words or phrases for a driving license (e.g. driving license, rijbewijs)

Netherlands IBAN Number Content Blade

The content blade requires the following to match for a Netherlands IBAN number in a close proximity.

1 IBAN words and phrases (e.g. International Bank Account Number, IBAN)

2 Netherlands IBAN number pattern

IBAN Rule: NL country code followed by 16 alphanumeric characters.

Pattern:

- NL*DDLLLLDDDDDDDDDD*
- NL DDLLLLDDDDDDDDDD
- NL *DD LLLL DDDDDDDDDD*
- NL *DD LLLL DDDD DDDD DD*
- NL*DD LLLL DDDD DDDD DD*
- NL*DDLLLL DDDD DDDDDD*
- NL*DD LLLL DDDDDDDDDD*
- NL DD LLLL D DD DD DD DDD
- NL *DD LLLL DD DD DD DDDD*
- NL *DD LLLL DDD DDDDDDD*
- NL *DD LLLL DDDD DD DD DD*

Spaces may be substituted with dashes

Netherlands National Identification Numbers Content Blade

The content blade requires the following to match for a Netherlands National Identification number in a close proximity.

1 Netherlands National Identification number (refer to entity description)

2 Words or phrases for a Netherlands National Identification number (e.g. sofinummer, burgerservicenummer)

Netherlands Passport Number Content Blade

The content blade requires the following to match for a Netherlands passport number in a close proximity.

1 Netherlands passport number (refer to entity description)

2 Words or phrases for a Netherlands passport number (e.g. paspoort , Noodpaspoort)

Nevada Drivers License Number Content Blade

The content blade looks for matches to the Nevada driver's license pattern and words and phrases such as driver's license and license number and terms such as NV or Nevada.

Driver's license pattern: 9 Numeric (SSN); or 12 Numeric (last 2 are year of birth), or 10 numeric

New Brunswick Drivers Licence Content Blade

The content blade looks for matches to the New Brunswick driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as NB or New Brunswick in a close proximity.

License pattern rules: 5 - 7 digits

Driver's license pattern:

- *DDDDD*
- *DDDDDD*
- *DDDDDDD*

New Hampshire Drivers License Number Content Blade

The content blade looks for matches to the New Hampshire driver's license pattern and words and phrases such as driver's license and license number and terms such as NH or New Hampshire.

Driver's license pattern: 2 Numeric, 3 Alphabetic, 5 Numeric

New Jersey Drivers License Number Content Blade

The content blade looks for matches to the New Jersey driver's license pattern and words and phrases such as driver's license and license number and terms such as NJ or New Jersey.

Driver's license pattern: 1 Alphabetic, 14 Numeric

New Mexico Drivers License Number Content Blade

The content blade looks for matches to the New Mexico driver's license pattern and words and phrases such as driver's license and license number and terms such as NM or New Mexico.

Driver's license pattern: 9 Numeric

New York Drivers License Number Content Blade

The content blade looks for matches to the New York driver's license pattern and words and phrases such as driver's license and license number and terms such as NY or New York.

Driver's license pattern: 9 Numeric

New Zealand Health Practitioner Index Number Content Blade

The content blade looks for matches to the New Zealand Health Practitioner Index entity and corroborative terms such as hpi-cpn or health practitioner index.

New Zealand Inland Revenue Department Number

The content blade looks for matches to the New Zealand Inland Revenue Department Number entity and words and phrases such as IRD Number or Inland Revenue Department Number.

New Zealand National Health Index Number Content Blade

The content blade looks for matches to the New Zealand National Health Index entity and corroborative terms such as nhi or National Health index.

Newfoundland and Labrador Drivers Licence Content Blade

The content blade looks for matches to the Newfoundland and Labrador driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as NL or Labrador in a close proximity.

License pattern rules: 1 letter followed by 9 digits

Driver's license pattern: *LDDDDDDDDD*

North Carolina Drivers License Number Content Blade

The content blade looks for matches to the North Carolina driver's license pattern and words and phrases such as driver's license and license number and terms such as NC or North Carolina.

Driver's license pattern: 6 - 8 Numeric

North Dakota Drivers License Number Content Blade

The content blade looks for matches to the North Dakota driver's license pattern and words and phrases such as driver's license and license number and terms such as ND or North Dakota.

Driver's license pattern: 9 Numeric; or 3 Alphabetic, 6 Numeric

Nova Scotia Drivers Licence Content Blade

The content blade looks for matches to the Nova Scotia driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as NS or Nova Scotia in a close proximity.

License pattern rules: 5 letters followed by 9 digits

Driver's license pattern: *LLLLDDDDDDDDD*

Ohio Drivers License Number Content Blade

The content blade looks for matches to the Ohio driver's license pattern and words and phrases such as driver's license and license number and terms such as OH or Ohio.

Driver's license pattern: 2 Alphabetic, 6 Numeric

Oklahoma License Number Content Blade

The content blade looks for matches to the Oklahoma driver's license pattern and words and phrases such as driver's license and license number and terms such as OK or Oklahoma.

Driver's license pattern: 1 Alphabetic, 8 Numeric; or 9 Numeric; or Social Security Number, Formatted

Ontario Drivers Licence Content Blade

The content blade looks for matches to the Ontario driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as ON or Ontario in a close proximity.

License pattern rules: 1 letter followed by 14 digits

Driver's license pattern: *LDDDDDDDDDDDDD*

Oregon License Number Content Blade

The content blade looks for matches to the Oregon driver's license pattern and words and phrases such as driver's license and license number and terms such as OR or Oregon.

Driver's license pattern: 6 -7 Numeric

Patient Identification Numbers Content Blade

This is a content blade that requires customization. To use this content blade, add a regular expression for a company-specific Patient Identification Number pattern. The content blade looks for matches to words and phrases such as patient id or a name, U.S. address or U.S. date in combination with the custom regular expression.

Pennsylvania License Number Content Blade

The content blade looks for matches to the Pennsylvania driver's license pattern and words and phrases such as driver's license and license number and terms such as PA or Pennsylvania.

Driver's license pattern: 8 Numeric

Prince Edward Island Drivers Licence Content Blade

The content blade looks for matches to the Prince Edward Island driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as PE or Prince Edward Island in a close proximity.

License pattern rules: 5 - 6 digits

Driver's license pattern:

- *DDDD*
- *DDDDDD*

Protected Health Information Terms Content Blade

The content blade looks for words and phrases related to personal health records and health insurance claims.

The content blade will match with a combination of the following pieces of information, either:

1 More than one match to the Protected Health Information dictionary

2 A single match to the Protected Health Information dictionary plus two of either a name, U.S. Address or U.S. Date

3 A single match to the Protected Health Information dictionary with a patient or doctor identification word or phrase (e.g. patient ID, physician name)

Quebec Drivers Licence Content Blade

The content blade looks for matches to the Quebec driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as QC or Quebec in a close proximity.

License pattern rules: 1 letter followed by 12 digits

Driver's license pattern: LDDDDDDDDDDDD

Rhode Island License Number Content Blade

The content blade looks for matches to the Rhode Island driver's license pattern and words and phrases such as driver's license and license number and terms such as RI or Rhode Island.

Driver's license pattern: 7 Numeric

Saskatchewan Drivers Licence Content Blade

The content blade looks for matches to the Saskatchewan driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as SK or Saskatchewan in a close proximity.

License pattern rules: 8 digits

License pattern: *DDDDDDDD*

SIN Formatted Content Blade

The content blade looks for formatted patterns of the Canadian Social Insurance number (SIN).

The content blade will match with a combination of the following pieces of information in medium proximity, either:

1 More than one match to a formatted SIN

2 A single match to a formatted SIN plus a driver's license or date of birth word or phrase

3 A single match to a formatted SIIN with word or p

SIN Unformatted Content Blade

The content blade looks for unformatted patterns of the Canadian Social Insurance (SIN). The content blade will match if an unformatted SIN is found within close proximity of a word or phrase for a Social Insurance number (e.g. Social Insurance, SIN) or driver's license or date of birth.

SSN Formatted Content Blade

SSN Formatted Content Blade

The content blade will match with a combination of the following pieces of information in medium proximity, either:

- More than one match to a formatted SSN
- A single match to a formatted SSN plus two of either a name, U.S. Address or U.S. Date
- A single match to a formatted SSN with word or phrase for a Social Security number (e.g. Social Security, SSN)

SSN Unformatted Content Blade

The content blade looks for unformatted patterns of the U.S. Social Security number (SSN). The content blade will match if an unformatted SSN is found within close proximity of a word or phrase for a Social Security number (e.g. Social Security, SSN).

South Carolina License Number Content Blade

The content blade looks for matches to the South Carolina driver's license pattern and words and phrases such as driver's license and license number and terms such as SC or South Carolina.

Driver's license pattern: 9 Numeric

South Dakota License Number Content Blade

The content blade looks for matches to the South Dakota driver's license pattern and words and phrases such as driver's license and license number and terms such as SD or South Dakota.

Driver's license pattern: 8 Numeric; or Social Security Number

Spain National Identification Number Content Blade

The content blade looks for matches to the Spain National Identification Number entity and words and phrases such as Documento Nacional de Identidad and Número de Identificación de Extranjeros. It also uses regular expressions to differentiate between telephone numbers and to prevent double counting of DNIs and NIEs without check letters.

Spain Passport Number Content Blade

The content blade looks for matches to the Spain Passport Number and words and phrases such as pasaporte or passport.

Passport Rule: 8 alphanumeric characters -- 2 letters followed by 6 digits.

Pattern:

LLDDDDDD

LL-DDDDDD

LL DDDDDD

Spain Social Security Number Content Blade

The content blade requires the following to match for a Spain Social Security number in a close proximity.

1 Spain Social Security number

2 Words or phrases for a social security number (e.g. número de la seguridad social, social security number)

Sweden IBAN Number Content Blade

The content blade requires the following to match for a Sweden IBAN number in a close proximity.

1 IBAN words and phrases (e.g. International Bank Account Number, IBAN

2 Sweden IBAN number pattern

IBAN Rule: SE country code followed by 22 digits.

Pattern: SE DDDDDDDDDDDDDDDDDDDDDD

Sweden Passport Number Content Blade

The content blade looks for matches to the Sweden Passport Number regular expression with the following possible combinations of supporting evidence.

1 Words and phrases for passport such as Passnummer

2 Words and phrases for the country Sweden, nationality and expiry dates

Passport Rule: 8 digits

Pattern:

DDDDDDDD

DD-DDDDDD

LL-DDDDDD

Tennessee License Number Content Blade

The content blade looks for matches to the Texas driver's license pattern and words and phrases such as driver's license and license number and terms such as TX or Texas.

Driver's license pattern: 8 Numeric

UK BIC Number Content Blade

The content blade scans for UK BIC numbers by requiring matches for both rules.

1 European BIC number format

2 UK format of the BIC number

BIC rule: 8 or 11 alphanumeric characters. Letters 5th and 6th will always have "GB" as the ISO 3166-1 alpha-2 country code.

Pattern:

LLLLLLAAA

LLLLLLAAAAA

LLLLLLAA-AAA

LLLLLLAA AAA

LLLLLL AA AAA

LLLL LL AA AAA

LLLL LL AA-AAA

UK Driving License Number Content Blade

The content blade requires the following to match for a UK driving license in a close proximity.

1 UK driving license pattern

2 Either words or phrases for a driving license (e.g. driving license) or personal identification (e.g. date of birth, address, telephone)

Driving license rule: 16 - 18 alphanumeric characters and begins with a letter.

Pattern:

LAAAADDDDDDLLDLLDD

Some digits are limited in the values accepted.

UK IBAN Number Content Blade

The content blade requires the following to match for a UK IBAN number in a close proximity.

1 European IBAN number format

2 UK IBAN number pattern

IBAN Rule: "GB" country code followed by 20 characters.

GB, ISO country code

2 Digits (numeric characters 0 to 9 only) , Check Digits (IBAN)

4 Upper case letters (A-Z only), Bank Identifier Digits

6 Digits (numeric characters 0 to 9 only), Bank branch code

8 Digits (numeric characters 0 to 9 only), Account number

Pattern:

GBDDLLLLDDDDDDDDDDDDDD

GB DD LLLL DDDD DDDD DDDD DD

GB DD LLLL DDDDDD DDDDDDDD

UK National Health Service Number Content Blade

The content blade requires the following to match for a UK National Health Service number in a close proximity.

1 UK National Health Service number format

2 Words and phrases relating to the National Health Service or patient identification or date of birth

UK NINO Formal Content Blade

The content blade looks for the formal pattern of the UK National Insurance number (NINO).

The content blade will match with a combination of the following pieces of information in high proximity, either:

1 More than one match to a NINO formal pattern

2 A single match to a NINO formal with word or phrase for a National Insurance number (e.g. NINO, taxpayer number)

UK Passport Number Content Blade

The content blade looks for matches to one of the U.K. passport number entities with the following supporting evidence.

1 Words and phrases for passport such as passport or a national passport code preceding a passport number

2 Words and phrases for the country, U.K, or the date of issue (optional match)

Utah License Number Content Blade

The content blade looks for matches to the Utah driver's license pattern and words and phrases such as driver's license and license number and terms such as UT or Utah.

Driver's license pattern: 6 - 10 Numeric

Virginia License Number Content Blade

The content blade looks for matches to the Virginia driver's license pattern and words and phrases such as driver's license and license number and terms such as VA or Virginia.

Driver's license pattern: 1 Alphabetic, 8 Numeric

Visa Card Number Content Blade

The content blade looks for a combination of the following pieces of information, either:

1 More than one JCB credit card number

2 A single credit card number plus words and phrases such as ccn, credit card, expiration date

3 A single credit card number plus an expiration date

Washington License Number Content Blade

The content blade looks for matches to the Washington driver's license pattern and words and phrases such as driver's license and license number and terms such as WA or Washington.

Driver's license pattern: 5 Alphabetic (last name), 1 Alphabetic (first name), 1 Alphabetic (middle name), 3 Numeric, 2 Alphanumeric. If last or middle name field falls short, fill with *s.

Wisconsin License Number Content Blade

The content blade looks for matches to the Wisconsin driver's license pattern and words and phrases such as driver's license and license number and terms such as WI or Wisconsin.

Driver's license pattern: 1 Alphabetic, 13 Numeric

Wyoming License Number Content Blade

The content blade looks for matches to the Wyoming driver's license pattern and words and phrases such as driver's license and license number and terms such as WY or Wyoming.

Driver's license pattern: 9 - 10 Numeric

Data Security Content Blades 17

This sections lists the available content blades for NSX regulations.

This chapter includes the following topics:

- "ABA Routing Number Content Blade," on page 260
- "Admittance and Discharge Dates Content Blade," on page 260
- "Alabama Drivers License Content Blade," on page 260
- "Alaska Drivers License Content Blade," on page 261
- "Alberta Drivers Licence Content Blade," on page 261
- "Alaska Drivers License Content Blade," on page 261
- "Alberta Drivers Licence Content Blade," on page 261
- "American Express Content Blade," on page 261
- "Arizona Drivers License Content Blade," on page 261
- "Arkansas Drivers License Content Blade," on page 262
- "Australia Bank Account Number Content Blade," on page 262
- "Australia Business Number Content Blade," on page 262
- "Australia Company Number Content Blade," on page 262
- "Australia Medicare Card Number Content Blade," on page 262
- "Australia Tax File Number Content Blade," on page 262
- "California Drivers License Number Content Blade," on page 263
- "Canada Drivers License Number Content Blade," on page 263
- "Canada Social Insurance Number Content Blade," on page 263
- "Colorado Drivers License Number Content Blade," on page 263
- "Connecticut Drivers License Number Content Blade," on page 263
- "Credit Card Number Content Blade," on page 263
- "Credit Card Track Data Content Blade," on page 263
- "Custom Account Number Content Blade," on page 264
- "Delaware Drivers License Number Content Blade," on page 264
- "EU Debit Card Number Content Blade," on page 264

- "Florida Drivers License Number Content Blade," on page 264
- "France Driving License Number Content Blade," on page 264
- "France BIC Number Content Blade," on page 264
- "France IBAN Number Content Blade," on page 264
- "France National Identification Number Content Blade," on page 265
- "France VAT Number Content Blade," on page 265
- "Georgia Drivers License Number Content Blade," on page 265
- "Germany BIC Number Content Blade," on page 265
- "Germany Driving License Number Content Blade," on page 265
- "Germany IBAN Number Content Blade," on page 265
- "Germany National Identification Numbers Content Blade," on page 265
- "Germany Passport Number Content Blade," on page 266
- "Germany VAT Number Content Blade," on page 266
- "Group Insurance Numbers Content Blade," on page 266
- "Hawaii Drivers License Number Content Blade," on page 266
- "Italy National Identification Numbers Content Blade," on page 266
- "Health Plan Beneficiary Numbers," on page 267
- "Idaho Drivers License Number Content Blade," on page 267
- "Illinois Drivers License Number Content Blade," on page 267
- "Indiana Drivers License Number Content Blade," on page 267
- "Iowa Drivers License Number Content Blade," on page 267
- "Index of Procedures Content Blade," on page 267
- "Italy Driving License Number Content Blade," on page 268
- "Italy IBAN Number Content Blade," on page 268
- "ITIN Unformatted Content Blade," on page 268
- "Kansas Drivers License Number Content Blade," on page 269
- "Kentucky Drivers License Number Content Blade," on page 269
- "Louisiana Drivers License Number Content Blade," on page 269
- "Maine Drivers License Number Content Blade," on page 269
- "Manitoba Drivers Licence Content Blade," on page 269
- "Maryland Drivers License Number Content Blade," on page 270
- "Massachusetts Drivers License Number Content Blade," on page 270
- "Michigan Drivers License Number Content Blade," on page 270
- "Minnesota Drivers License Number Content Blade," on page 270
- "Mississippi Drivers License Number Content Blade," on page 270
- "Missouri Drivers License Number Content Blade," on page 270
- "Montana Drivers License Number Content Blade," on page 270

- "NDC Formulas Dictionary Content Blade," on page 270
- "Nebraska Drivers License Number Content Blade," on page 271
- "Netherlands Driving Licence Number Content Blade," on page 271
- "Netherlands IBAN Number Content Blade," on page 271
- "Netherlands National Identification Numbers Content Blade," on page 271
- "Netherlands Passport Number Content Blade," on page 272
- "Nevada Drivers License Number Content Blade," on page 272
- "New Brunswick Drivers Licence Content Blade," on page 272
- "New Hampshire Drivers License Number Content Blade," on page 272
- "New Jersey Drivers License Number Content Blade," on page 272
- "New Mexico Drivers License Number Content Blade," on page 272
- "New York Drivers License Number Content Blade," on page 272
- "New Zealand Health Practitioner Index Number Content Blade," on page 273
- "New Zealand Inland Revenue Department Number," on page 273
- "New Zealand National Health Index Number Content Blade," on page 273
- "Newfoundland and Labrador Drivers Licence Content Blade," on page 273
- "North Carolina Drivers License Number Content Blade," on page 273
- "North Dakota Drivers License Number Content Blade," on page 273
- "Nova Scotia Drivers Licence Content Blade," on page 273
- "Ohio Drivers License Number Content Blade," on page 273
- "Oklahoma License Number Content Blade," on page 274
- "Ontario Drivers Licence Content Blade," on page 274
- "Oregon License Number Content Blade," on page 274
- "Patient Identification Numbers Content Blade," on page 274
- "Pennsylvania License Number Content Blade," on page 274
- "Prince Edward Island Drivers Licence Content Blade," on page 274
- "Protected Health Information Terms Content Blade," on page 274
- "Quebec Drivers Licence Content Blade," on page 275
- "Rhode Island License Number Content Blade," on page 275
- "Saskatchewan Drivers Licence Content Blade," on page 275
- "SIN Formatted Content Blade," on page 275
- "SIN Unformatted Content Blade," on page 275
- "SSN Formatted Content Blade," on page 275
- "SSN Unformatted Content Blade," on page 276
- "South Carolina License Number Content Blade," on page 276
- "South Dakota License Number Content Blade," on page 276
- "Spain National Identification Number Content Blade," on page 276

- "Spain Passport Number Content Blade," on page 276
- "Spain Social Security Number Content Blade," on page 276
- "Sweden IBAN Number Content Blade," on page 276
- "Sweden Passport Number Content Blade," on page 277
- "Tennessee License Number Content Blade," on page 277
- "UK BIC Number Content Blade," on page 277
- "UK Driving License Number Content Blade," on page 277
- "UK IBAN Number Content Blade," on page 278
- "UK National Health Service Number Content Blade," on page 278
- "UK NINO Formal Content Blade," on page 278
- "UK Passport Number Content Blade," on page 278
- "Utah License Number Content Blade," on page 279
- "Virginia License Number Content Blade," on page 279
- "Visa Card Number Content Blade," on page 279
- "Washington License Number Content Blade," on page 279
- "Wisconsin License Number Content Blade," on page 279
- "Wyoming License Number Content Blade," on page 279

ABA Routing Number Content Blade

The content blade looks for matches to 3 pieces of information in close proximity of each other.

The content blade looks for:

- ABA routing number
- Banking words and phrases (e.g. aba, routing number, checking, savings)
- Personally identifiable information (e.g. name, address, phone number)

Words and phrases related to banking are implemented in order to increase precision. A routing number is 9-digits and may pass for many different data types, for example, a valid US Social Security number, Canadian Social Insurance number or international telephone number.

Since routing numbers themselves are not sensitive, personally identifiable information is necessary for a violation to occur.

Admittance and Discharge Dates Content Blade

The content blade looks for matches to the U. S. Date Format entity and words and phrases such as admit date, admittance date, date of discharge, discharge date in close proximity to each other.

Alabama Drivers License Content Blade

The content blade looks for matches to the Alabama driver's license pattern and words and phrases such as driver's license and license number and, optionally, terms such as AL or Alabama.

Driver's license pattern

7 Numeric or 8 Numeric

Alaska Drivers License Content Blade

The content blade looks for matches to the Alaska driver’s license pattern and words and phrases such as driver’s license and license number and, optionally, terms such as AK or Alaska.

Driver's license pattern:

7 Numeric

Alberta Drivers Licence Content Blade

The content blade looks for matches to the Alberta driver’s license pattern and words and phrases such as driver’s license and license number and, optionally, terms such as AK or Alberta.

Driver's license pattern

7 Numeric

Alaska Drivers License Content Blade

The content blade looks for matches to the Alaska driver’s license pattern and words and phrases such as driver’s license and license number and, optionally, terms such as AK or Alaska.

Driver's license pattern:

7 Numeric

Alberta Drivers Licence Content Blade

The content blade looks for matches to the Alberta driver’s license pattern and words and phrases such as driver’s license and license number and, optionally, terms such as AK or Alberta.

Driver's license pattern

7 Numeric

American Express Content Blade

The content blade looks for a combination of the following pieces of information.

- More than one American Express credit card number
- A single credit card number plus words and phrases such as ccn, credit card, expiration date
- A single credit card number plus an expiration date

Arizona Drivers License Content Blade

The content blade looks for matches to the Arizona driver’s license pattern and words and phrases such as driver’s license and license number and, optionally, terms such as AZ or Arizona.

The Driver's license pattern can be 1 Alphabetic, 8 Numeric; or 9 Numeric (SSN); or 9 Numeric (Unformatted SSN).

Arkansas Drivers License Content Blade

The content blade looks for matches to the Arkansas driver's license pattern and words and phrases such as driver's license and license number and, optionally, terms such as AR or Arkansas.

Driver's license pattern can be 9, 8 Numeric.

Australia Bank Account Number Content Blade

The Australian bank account number itself is not sensitive, but identifies a bank account, without identifying the bank branch. Therefore, both the account number and branch information must exist for the document to be considered sensitive.

The content blade looks for matches to both:

- An Australian bank account number
- Words and phrases related to bank state branch or BSB.

It also uses a regular expression rule to differentiate between telephone numbers of the same length.

An Australian bank account number is 6 to 10-digits without any embedded meaning. It has no check digit routine.

Australia Business Number Content Blade

The content blade looks for matches to both pieces of information in close proximity to each other.

- Australia Business Number
- ABN words and phrases (e.g. ABN, Australia business number)

Australia Company Number Content Blade

The content blade looks for matches to both pieces of information in close proximity to each other.

- Australia Company Number
- ACN words and phrases (e.g. ACN, Australia Company Number)

Australia Medicare Card Number Content Blade

The content blade will match if one of the following combinations of information appears in a document.

- More than one Australia Medicare Card Number
- One Medicare card number plus Medicare or patient identification terms (e.g. patient identifier, patient number)
- One Medicare card number plus two of either a name, expiration date or expiration terms

Australia Tax File Number Content Blade

The content blade looks for matches to both pieces of information in high proximity to each other.

- Australia Tax File Number (refer to entity description)
- Tax file number words and phrases (e.g. TFN, tax file number)

California Drivers License Number Content Blade

The content blade looks for matches to the California driver's license pattern and words and phrases such as driver's license and license number and terms such as CA or California.

The Driver's license pattern is 1 Alphabetic, 7 Numeric.

Canada Drivers License Number Content Blade

The content blade is only a container file for child content blades. The content blades assigned to it separately look for driver's licenses in individual providences and territories.

Canada Social Insurance Number Content Blade

The content blade is only a container file for child content blades. The content blades assigned to it separately look for formatted and unformatted versions of the Canadian Social Insurance numbers plus personal information so different rules may be assigned to them. The formatted version of the Social Insurance number is a more specific pattern, so the rules are less strict for retuning a match. However, the unformatted version is very general and matches to many common numbers.

Colorado Drivers License Number Content Blade

The content blade looks for matches to the Colorado driver's license pattern and words and phrases such as driver's license and license number and terms such as CO or Colorado.

The driver's license pattern is 9 Numeric.

Connecticut Drivers License Number Content Blade

The content blade looks for matches to the Connecticut driver's license pattern and words and phrases such as driver's license and license number and terms such as CT or Connecticut.

Driver's license pattern: 9 Numeric, 1st two positions are month of birth in odd or even year. 01-12 Jan-Dec odd years, 13-24 Jan-Dec even years, 99 unknown.

Credit Card Number Content Blade

The content blade looks for a combination of the following pieces of information.

- More than one credit card number
- A single credit card number plus words and phrases such as ccn, credit card, expiration date
- A single credit card number plus an expiration date

Credit Card Track Data Content Blade

Track data is the information encoded and stored on two tracks located within the magnetic stripe on the back of a credit card (debit card, gift card, etc). There are three tracks on the magstripe (magnetic strip on the back of a credit card).

Each track is .110-inch wide. The ISO/IEC standard 7811, which is used by banks, specifies:

- Track one is 210 bits per inch (bpi), and holds 79 six-bit plus parity bit read-only characters.
- Track two is 75 bpi, and holds 40 four-bit plus parity bit characters.
- Track three is 210 bpi, and holds 107 four-bit plus parity bit characters.

Your credit card typically uses only tracks one and two. Track three is a read/write track (that includes an encrypted PIN, country code, currency units, amount authorized), but its usage is not standardized among banks.

This content blade requires a match to the Credit Card Track Data entity.

Custom Account Number Content Blade

The Custom Accounts content blade is an editable blade and should contain a regular expression for an organization's custom account patterns.

Delaware Drivers License Number Content Blade

The content blade looks for matches to the Delaware driver's license pattern and words and phrases such as driver's license and license number and terms such as DE or Delaware.

EU Debit Card Number Content Blade

The content blade looks for patterns of the major European Union debit card numbers.

The content blade will match with a combination of the following pieces of information in close proximity, if either:

- More than one match to a EU debit card number
- A single match to a EU debit card number plus two of either a word or phrase for credit card (e.g. card number or cc#), credit card security, expiration date or name
- A single match to a EU debit card number with an expiration date

Florida Drivers License Number Content Blade

The content blade looks for matches to the Florida driver's license pattern and words and phrases such as driver's license and license number and terms such as FL or Florida.

Driver's license pattern: 1 Alphabetic, 12 Numeric.

France Driving License Number Content Blade

The content blade requires the following to match for a French driving license in a close proximity.

- French driving license pattern
- Either words or phrases for a driving license (e.g. driving license, permis de conduire) or E.U. date format

France BIC Number Content Blade

The content blade scans for French BIC numbers by requiring matches for both the following rules.

- European BIC number format
- French format of the BIC number

France IBAN Number Content Blade

The content blade requires the following to match for a French IBAN number in a close proximity.

- European IBAN number format
- French IBAN number pattern

France National Identification Number Content Blade

The content blade requires the following to match for a French National Identification number in a close proximity.

- More than one match to the French National Identification pattern
- One match to the French National Identification pattern plus either words or phrases for a social security number (e

France VAT Number Content Blade

The content blade requires a match for a French value added tax (VAT) number pattern in a close proximity to the abbreviation FR.

Georgia Drivers License Number Content Blade

The content blade looks for matches to the Georgia driver's license pattern and words and phrases such as driver's license and license number and terms such as GA or Georgia.

Driver's license pattern: 7-9 Numeric; or Formatted SSN.

Germany BIC Number Content Blade

The content blade scans for German BIC numbers by requiring matches for both the following rules.

- European BIC number format
- German format of the BIC number

Germany Driving License Number Content Blade

The content blade requires the following to match for a German driving license in a close proximity.

- German driving license pattern
- Words or phrases related to a driving license (e.g. driving license, ausstellungsdatum)

Germany IBAN Number Content Blade

The content blade requires the following to match for a German IBAN number in a close proximity.

- European IBAN number format
- German IBAN number pattern

THe German IBAN rule: "DE" country code followed by 22 digits.

Germany National Identification Numbers Content Blade

The content blade requires the following to match for a German National Identification number in a close proximity.

- Either a German National Identification number or a machine-readable version of the number
- Words or phrases for a German National Identification number (e.g. personalausweis, personalausweisnummer)

Germany Passport Number Content Blade

The content blade requires the following to match for a German passport number in a close proximity.

- Either a German passport number or a machine-readable version of the number
- Words or phrases for a German passport number or issuance date (e.g. reisepass, ausstellungsdatum)

Germany VAT Number Content Blade

The content blade requires a match for a German value added tax (VAT) number pattern (refer to entity description) in a close proximity to the abbreviation DE.

Group Insurance Numbers Content Blade

This is a content blade that requires customization. To use this content blade, add a regular expression to match the number pattern for an organization's Group Insurance Number. The content blade looks for matches to words and phrases such as group insurance or a name, U.S. address or U.S. date in combination with the custom regular expression.

Hawaii Drivers License Number Content Blade

The content blade looks for matches to the Hawaii driver's license pattern and words and phrases such as driver's license and license number and terms such as HI or Hawaii.

Driver's license pattern: H Alphabetic, 8 Numeric; or SSN.

Italy National Identification Numbers Content Blade

The content blade requires the following to match for an Italy National Identification number in a close proximity.

1 Italy National Identification number pattern

2 Words or phrases for an Italy National Identification number (e.g. codice fiscale, national identification)

National Identification Rule: 16 character alphanumeric code. where:

- *SSS* are the first three consonants in the family name (the first vowel and then an X are used if there are not enough consonants)
- *NNN* is the first name, of which the first, third and fourth consonants are used—exceptions are handled as in family names
- *YY* are the last digits of the birth year
- *M* is the letter for the month of birth—letters are used in alphabetical order, but only the letters A to E, H, L, M, P, R to T are used (thus, January is A and October is R)
- *DD* is the day of the month of birth—in order to differentiate between genders, 40 is added to the day of birth for women (thus a woman born on May 3 has ...E43...)
- *ZZZZ* is an area code specific to the municipality where the person was born—country-wide codes are used for foreign countries, a letter followed by three digits

- *X* is a parity character as calculated by adding together characters in the even and odd positions, and dividing them by 26. Numerical values are used for letters in even positions according to their alphabetical order. Characters in odd positions have different values. A letter is then used which corresponds to the value of the remainder of the division in the alphabet.

Pattern:

- *LLLLLLDDLDDLDDDL*
- *LLL LLL DDLDD LDDDL*

Health Plan Beneficiary Numbers

This is a content blade that requires customization. To use this content blade, add a regular expression to identify recipients of health plan benefits and payments. The content blade looks for matches to words and phrases such as beneficiary or a name, U.S. address or U.S. date in combination with the custom regular expression.

Idaho Drivers License Number Content Blade

The content blade looks for matches to the Idaho driver's license pattern and words and phrases such as driver's license and license number and terms such as ID or Idaho.

Driver's license pattern: 2 Alphabetic, 6 Numeric, 1 Alphabetic.

Illinois Drivers License Number Content Blade

The content blade looks for matches to the Illinois driver's license pattern and words and phrases such as driver's license and license number and terms such as IL or Illinois.

Driver's license pattern: 1 Alphabetic, 11 Numeric.

Indiana Drivers License Number Content Blade

The content blade looks for matches to the Indiana driver's license pattern and words and phrases such as driver's license and license number and terms such as IN or Indiana.

Driver's license pattern: 10 Numeric.

Iowa Drivers License Number Content Blade

The content blade looks for matches to the Iowa driver's license pattern and words and phrases such as driver's license and license number and terms such as IA or Iowa.

Driver's license pattern can be 3 numeric, 2 alphabetic, 3 numeric; or Social Security Number.

Index of Procedures Content Blade

The content blade looks for words and phrases related to medical procedures based on the International Classification of Diseases (ICD).

The content blade will match with a combination of the following pieces of information, either:

- More than one match to the Index of Procedures dictionary
- A single match to the Index of Procedures dictionary plus two of either a name, U.S. Address or U.S. Date
- A single match to the Index of Procedures dictionary with a patient or doctor identification word or phrase (e.g. patient ID, physician name)

Italy Driving License Number Content Blade

The content blade requires the following to match for an Italy driving license in a close proximity.

- Italy driving license pattern
- Words or phrases for a driving license (e.g. driving license, patente di guida)

Driver's License Rule: 10 alphanumeric characters -- 2 letters, 7 numbers and a final letter. The first letter may only be characters A-V.

Driver's License Pattern:

- *LLDDDDDDDL*
- *LL DDDDDDD* L
- *LL-DDDDDDD-L*
- *LL - DDDDDDD - L*

Italy IBAN Number Content Blade

The content blade requires the following to match for a Italy IBAN number in a close proximity.

1 IBAN words and phrases (e.g. International Bank Account Number, IBAN)

2 Italy IBAN number pattern

IBAN Rule: IT country code followed by 25 alphanumeric characters.

Pattern:

- IT*DDLDDDDDDDDDDAAAAAAAAAAAA*
- IT *DDL DDDDD DDDDD AAAAAAAAAAA*
- IT *DD LDDDDD DDDDD AAAAAAAAAAA*
- IT *DD L DDDDD DDDDD AAAAAAAAAAA*
- IT *DD LDDDDDDDDDDAAAAAAAAAAA*
- IT *DD L DDDDDDDDDDAAAAAAAAAAA*
- IT*DD LDDD DDDD DDDA AAAA AAAA AAA*
- IT *DDL DDDDD DDDDD AAAAAA AAAAAA*
- IT *DDL DDD DDD DDD DAAA AAA AAAAAA*
- IT *DDL DDDDDDDDDD AAAAAA AAAAAA*

Spaces may be substituted with dashes, forward slashes or colons.

ITIN Unformatted Content Blade

The content blade looks for unformatted patterns of the U.S. Taxpayer Identification Number (ITIN). The content blade will match if an unformatted ITIN is found within close proximity of a word or phrase for an ITIN number (e.g. tax identification, ITIN).

ITIN Rule: 9-digit number that always begins with the number 9 and has a range of 70-88 in the fourth and fifth digit.

Pattern: *DDDDDDDDD*

Kansas Drivers License Number Content Blade

The content blade looks for matches to the Kansas driver's license pattern and words and phrases such as driver's license and license number and terms such as KS or Kansas.

Driver's license pattern: 1 Alphabetic (K), 8 Numeric; or Social Security Number.

Kentucky Drivers License Number Content Blade

The content blade looks for matches to the Kentucky driver's license pattern and words and phrases such as driver's license and license number and terms such as KY or Kentucky.

Driver's license pattern: 1 Alphabetic, 8 Numeric; or Social Security Number.

Louisiana Drivers License Number Content Blade

The content blade looks for matches to the Louisiana driver's license pattern and words and phrases such as driver's license and license number and terms such as LA or Louisiana.

Driver's license pattern: 2 Zeros, 7 Numeric.

Maine Drivers License Number Content Blade

The content blade looks for matches to the Maine driver's license pattern and words and phrases such as driver's license and license number and terms such as ME or Maine.

Driver's license pattern: 7 Numeric, optional alphabetic X.

Manitoba Drivers Licence Content Blade

The content blade looks for matches to the Manitoba driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as MB or Manitoba in a close proximity.

License pattern rules: 12 alphanumeric characters that may be hyphen-separated, where:

- 1st character is a letter
- 2nd - 5th characters are a letter or asterisk
- 6th character is a letter
- 7th - 10th characters are digits
- 11th character is a letter
- 12th character is a letter or digit

or

- 1st character is a letter
- 2nd - 4th characters are a letter or asterisk
- 5th - 6th characters are digits
- 7th - 12th characters are a letter or digit

Driver's license pattern:

- *LLLLLLDDDDLA*
- *LLLLLDDAAAAAA*

Maryland Drivers License Number Content Blade

The content blade looks for matches to the Maryland driver's license pattern and words and phrases such as driver's license and license number and terms such as MD or Maryland.

Driver's license pattern: 1 Alphabetic, 12 Numeric

Massachusetts Drivers License Number Content Blade

The content blade looks for matches to the Massachusetts driver's license pattern and words and phrases such as driver's license and license number and terms such as MA or Massachusetts.

Driver's license pattern: 1 Alphabetic (S), 8 Numeric; or Social Security Number

Michigan Drivers License Number Content Blade

The content blade looks for matches to the Michigan driver's license pattern and words and phrases such as driver's license and license number and terms such as MI or Michigan.

Driver's license pattern: 1 Alphabetic, 12 Numeric

Minnesota Drivers License Number Content Blade

The content blade looks for matches to the Minnesota driver's license pattern and words and phrases such as driver's license and license number and terms such as MN or Minnesota.

Driver's license pattern: 1 Alphabetic, 12 Numeric

Mississippi Drivers License Number Content Blade

The content blade looks for matches to the Mississippi driver's license pattern and words and phrases such as driver's license and license number and terms such as MS or Mississippi.

Driver's license pattern: 9 Numeric; or Formatted Social Security Number

Missouri Drivers License Number Content Blade

The content blade looks for matches to the Missouri driver's license pattern and words and phrases such as driver's license and license number and terms such as MO or Missouri

Driver's license pattern: 1 Alphabetic, 6-9 Numeric; or 9 Numeric; or Formatted Social Security Number

Montana Drivers License Number Content Blade

The content blade looks for matches to the Montana driver's license pattern and words and phrases such as driver's license and license number and terms such as MT or Montana.

Driver's license pattern: 9 Numeric (SSN); or 1 Alphabetic, 1 Numeric, 1 Alphanumeric, 2 Numeric, 3 Alphabetic and 1 Numeric; or 13 Numeric

NDC Formulas Dictionary Content Blade

The content blade looks for words and phrases related to formulas based on the National Drug Codes (NDC).

The content blade will match with a combination of the following pieces of information, either:

1 More than one match to the NDC Formulas dictionary

2 A single match to the NDC Formulas dictionary plus two of either a name, U.S. Address or U.S. Date

3 A single match to the NDC Formulas dictionary with a patient or doctor identification word or phrase (e.g. patient ID, physician name)

Nebraska Drivers License Number Content Blade

The content blade looks for matches to the Nebraska driver's license pattern and words and phrases such as driver's license and license number and terms such as NE or Nebraska.

Driver's license pattern: 1 Alphabetic , 8 Numeric

Netherlands Driving Licence Number Content Blade

The content blade requires the following to match for a Netherlands driving license in a close proximity.

1 Netherlands driving license pattern (refer to entity description)

2 Words or phrases for a driving license (e.g. driving license, rijbewijs)

Netherlands IBAN Number Content Blade

The content blade requires the following to match for a Netherlands IBAN number in a close proximity.

1 IBAN words and phrases (e.g. International Bank Account Number, IBAN)

2 Netherlands IBAN number pattern

IBAN Rule: NL country code followed by 16 alphanumeric characters.

Pattern:

- NL*DDLLLLDDDDDDDDDD*
- NL DDLLLLDDDDDDDDDD
- NL *DD LLLL DDDDDDDDDD*
- NL *DD LLLL DDDD DDDD DD*
- NL*DD LLLL DDDD DDDD DD*
- NL*DDLLLL DDDD DDDDDD*
- NL*DD LLLL DDDDDDDDDD*
- NL DD LLLL D DD DD DD DDD
- NL *DD LLLL DD DD DD DDDD*
- NL *DD LLLL DDD DDDDDDD*
- NL *DD LLLL DDDD DD DD DD*

Spaces may be substituted with dashes

Netherlands National Identification Numbers Content Blade

The content blade requires the following to match for a Netherlands National Identification number in a close proximity.

1 Netherlands National Identification number (refer to entity description)

2 Words or phrases for a Netherlands National Identification number (e.g. sofinummer, burgerservicenummer)

Netherlands Passport Number Content Blade

The content blade requires the following to match for a Netherlands passport number in a close proximity.

1 Netherlands passport number (refer to entity description)

2 Words or phrases for a Netherlands passport number (e.g. paspoort , Noodpaspoort)

Nevada Drivers License Number Content Blade

The content blade looks for matches to the Nevada driver's license pattern and words and phrases such as driver's license and license number and terms such as NV or Nevada.

Driver's license pattern: 9 Numeric (SSN); or 12 Numeric (last 2 are year of birth), or 10 numeric

New Brunswick Drivers Licence Content Blade

The content blade looks for matches to the New Brunswick driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as NB or New Brunswick in a close proximity.

License pattern rules: 5 - 7 digits

Driver's license pattern:

- *DDDDD*
- *DDDDDD*
- *DDDDDDD*

New Hampshire Drivers License Number Content Blade

The content blade looks for matches to the New Hampshire driver's license pattern and words and phrases such as driver's license and license number and terms such as NH or New Hampshire.

Driver's license pattern: 2 Numeric, 3 Alphabetic, 5 Numeric

New Jersey Drivers License Number Content Blade

The content blade looks for matches to the New Jersey driver's license pattern and words and phrases such as driver's license and license number and terms such as NJ or New Jersey.

Driver's license pattern: 1 Alphabetic, 14 Numeric

New Mexico Drivers License Number Content Blade

The content blade looks for matches to the New Mexico driver's license pattern and words and phrases such as driver's license and license number and terms such as NM or New Mexico.

Driver's license pattern: 9 Numeric

New York Drivers License Number Content Blade

The content blade looks for matches to the New York driver's license pattern and words and phrases such as driver's license and license number and terms such as NY or New York.

Driver's license pattern: 9 Numeric

New Zealand Health Practitioner Index Number Content Blade

The content blade looks for matches to the New Zealand Health Practitioner Index entity and corroborative terms such as hpi-cpn or health practitioner index.

New Zealand Inland Revenue Department Number

The content blade looks for matches to the New Zealand Inland Revenue Department Number entity and words and phrases such as IRD Number or Inland Revenue Department Number.

New Zealand National Health Index Number Content Blade

The content blade looks for matches to the New Zealand National Health Index entity and corroborative terms such as nhi or National Health index.

Newfoundland and Labrador Drivers Licence Content Blade

The content blade looks for matches to the Newfoundland and Labrador driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as NL or Labrador in a close proximity.

License pattern rules: 1 letter followed by 9 digits

Driver's license pattern: *LDDDDDDDDD*

North Carolina Drivers License Number Content Blade

The content blade looks for matches to the North Carolina driver's license pattern and words and phrases such as driver's license and license number and terms such as NC or North Carolina.

Driver's license pattern: 6 - 8 Numeric

North Dakota Drivers License Number Content Blade

The content blade looks for matches to the North Dakota driver's license pattern and words and phrases such as driver's license and license number and terms such as ND or North Dakota.

Driver's license pattern: 9 Numeric; or 3 Alphabetic, 6 Numeric

Nova Scotia Drivers Licence Content Blade

The content blade looks for matches to the Nova Scotia driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as NS or Nova Scotia in a close proximity.

License pattern rules: 5 letters followed by 9 digits

Driver's license pattern: *LLLLDDDDDDDDD*

Ohio Drivers License Number Content Blade

The content blade looks for matches to the Ohio driver's license pattern and words and phrases such as driver's license and license number and terms such as OH or Ohio.

Driver's license pattern: 2 Alphabetic, 6 Numeric

Oklahoma License Number Content Blade

The content blade looks for matches to the Oklahoma driver's license pattern and words and phrases such as driver's license and license number and terms such as OK or Oklahoma.

Driver's license pattern: 1 Alphabetic, 8 Numeric; or 9 Numeric; or Social Security Number, Formatted

Ontario Drivers Licence Content Blade

The content blade looks for matches to the Ontario driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as ON or Ontario in a close proximity.

License pattern rules: 1 letter followed by 14 digits

Driver's license pattern: *LDDDDDDDDDDDDD*

Oregon License Number Content Blade

The content blade looks for matches to the Oregon driver's license pattern and words and phrases such as driver's license and license number and terms such as OR or Oregon.

Driver's license pattern: 6 -7 Numeric

Patient Identification Numbers Content Blade

This is a content blade that requires customization. To use this content blade, add a regular expression for a company-specific Patient Identification Number pattern. The content blade looks for matches to words and phrases such as patient id or a name, U.S. address or U.S. date in combination with the custom regular expression.

Pennsylvania License Number Content Blade

The content blade looks for matches to the Pennsylvania driver's license pattern and words and phrases such as driver's license and license number and terms such as PA or Pennsylvania.

Driver's license pattern: 8 Numeric

Prince Edward Island Drivers Licence Content Blade

The content blade looks for matches to the Prince Edward Island driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as PE or Prince Edward Island in a close proximity.

License pattern rules: 5 - 6 digits

Driver's license pattern:

- *DDDD*
- *DDDDDD*

Protected Health Information Terms Content Blade

The content blade looks for words and phrases related to personal health records and health insurance claims.

The content blade will match with a combination of the following pieces of information, either:

1 More than one match to the Protected Health Information dictionary

2 A single match to the Protected Health Information dictionary plus two of either a name, U.S. Address or U.S. Date

3 A single match to the Protected Health Information dictionary with a patient or doctor identification word or phrase (e.g. patient ID, physician name)

Quebec Drivers Licence Content Blade

The content blade looks for matches to the Quebec driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as QC or Quebec in a close proximity.

License pattern rules: 1 letter followed by 12 digits

Driver's license pattern: LDDDDDDDDDDDD

Rhode Island License Number Content Blade

The content blade looks for matches to the Rhode Island driver's license pattern and words and phrases such as driver's license and license number and terms such as RI or Rhode Island.

Driver's license pattern: 7 Numeric

Saskatchewan Drivers Licence Content Blade

The content blade looks for matches to the Saskatchewan driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as SK or Saskatchewan in a close proximity.

License pattern rules: 8 digits

License pattern: *DDDDDDDD*

SIN Formatted Content Blade

The content blade looks for formatted patterns of the Canadian Social Insurance number (SIN).

The content blade will match with a combination of the following pieces of information in medium proximity, either:

1 More than one match to a formatted SIN

2 A single match to a formatted SIN plus a driver's license or date of birth word or phrase

3 A single match to a formatted SIIN with word or p

SIN Unformatted Content Blade

The content blade looks for unformatted patterns of the Canadian Social Insurance (SIN). The content blade will match if an unformatted SIN is found within close proximity of a word or phrase for a Social Insurance number (e.g. Social Insurance, SIN) or driver's license or date of birth.

SSN Formatted Content Blade

SSN Formatted Content Blade

The content blade will match with a combination of the following pieces of information in medium proximity, either:

- More than one match to a formatted SSN
- A single match to a formatted SSN plus two of either a name, U.S. Address or U.S. Date
- A single match to a formatted SSN with word or phrase for a Social Security number (e.g. Social Security, SSN)

SSN Unformatted Content Blade

The content blade looks for unformatted patterns of the U.S. Social Security number (SSN). The content blade will match if an unformatted SSN is found within close proximity of a word or phrase for a Social Security number (e.g. Social Security, SSN).

South Carolina License Number Content Blade

The content blade looks for matches to the South Carolina driver's license pattern and words and phrases such as driver's license and license number and terms such as SC or South Carolina.

Driver's license pattern: 9 Numeric

South Dakota License Number Content Blade

The content blade looks for matches to the South Dakota driver's license pattern and words and phrases such as driver's license and license number and terms such as SD or South Dakota.

Driver's license pattern: 8 Numeric; or Social Security Number

Spain National Identification Number Content Blade

The content blade looks for matches to the Spain National Identification Number entity and words and phrases such as Documento Nacional de Identidad and Número de Identificación de Extranjeros. It also uses regular expressions to differentiate between telephone numbers and to prevent double counting of DNIs and NIEs without check letters.

Spain Passport Number Content Blade

The content blade looks for matches to the Spain Passport Number and words and phrases such as pasaporte or passport.

Passport Rule: 8 alphanumeric characters -- 2 letters followed by 6 digits.

Pattern:

LLDDDDDD

LL-DDDDDD

LL DDDDDD

Spain Social Security Number Content Blade

The content blade requires the following to match for a Spain Social Security number in a close proximity.

1 Spain Social Security number

2 Words or phrases for a social security number (e.g. número de la seguridad social, social security number)

Sweden IBAN Number Content Blade

The content blade requires the following to match for a Sweden IBAN number in a close proximity.

1 IBAN words and phrases (e.g. International Bank Account Number, IBAN

2 Sweden IBAN number pattern

IBAN Rule: SE country code followed by 22 digits.

Pattern: SE DDDDDDDDDDDDDDDDDDDDDD

Sweden Passport Number Content Blade

The content blade looks for matches to the Sweden Passport Number regular expression with the following possible combinations of supporting evidence.

1 Words and phrases for passport such as Passnummer

2 Words and phrases for the country Sweden, nationality and expiry dates

Passport Rule: 8 digits

Pattern:

DDDDDDDD

DD-DDDDDD

LL-DDDDDD

Tennessee License Number Content Blade

The content blade looks for matches to the Texas driver's license pattern and words and phrases such as driver's license and license number and terms such as TX or Texas.

Driver's license pattern: 8 Numeric

UK BIC Number Content Blade

The content blade scans for UK BIC numbers by requiring matches for both rules.

1 European BIC number format

2 UK format of the BIC number

BIC rule: 8 or 11 alphanumeric characters. Letters 5th and 6th will always have "GB" as the ISO 3166-1 alpha-2 country code.

Pattern:

LLLLLLAAA

LLLLLLAAAAA

LLLLLLAA-AAA

LLLLLLAA AAA

LLLLLL AA AAA

LLLL LL AA AAA

LLLL LL AA-AAA

UK Driving License Number Content Blade

The content blade requires the following to match for a UK driving license in a close proximity.

1 UK driving license pattern

2 Either words or phrases for a driving license (e.g. driving license) or personal identification (e.g. date of birth, address, telephone)

Driving license rule: 16 - 18 alphanumeric characters and begins with a letter.

Pattern:

LAAAADDDDDDLLDLLDD

Some digits are limited in the values accepted.

UK IBAN Number Content Blade

The content blade requires the following to match for a UK IBAN number in a close proximity.

1 European IBAN number format

2 UK IBAN number pattern

IBAN Rule: "GB" country code followed by 20 characters.

GB, ISO country code

2 Digits (numeric characters 0 to 9 only) , Check Digits (IBAN)

4 Upper case letters (A-Z only), Bank Identifier Digits

6 Digits (numeric characters 0 to 9 only), Bank branch code

8 Digits (numeric characters 0 to 9 only), Account number

Pattern:

GBDDLLLLDDDDDDDDDDDDDD

GB DD LLLL DDDD DDDD DDDD DD

GB DD LLLL DDDDDD DDDDDDDD

UK National Health Service Number Content Blade

The content blade requires the following to match for a UK National Health Service number in a close proximity.

1 UK National Health Service number format

2 Words and phrases relating to the National Health Service or patient identification or date of birth

UK NINO Formal Content Blade

The content blade looks for the formal pattern of the UK National Insurance number (NINO).

The content blade will match with a combination of the following pieces of information in high proximity, either:

1 More than one match to a NINO formal pattern

2 A single match to a NINO formal with word or phrase for a National Insurance number (e.g. NINO, taxpayer number)

UK Passport Number Content Blade

The content blade looks for matches to one of the U.K. passport number entities with the following supporting evidence.

1 Words and phrases for passport such as passport or a national passport code preceding a passport number

2 Words and phrases for the country, U.K, or the date of issue (optional match)

Utah License Number Content Blade

The content blade looks for matches to the Utah driver's license pattern and words and phrases such as driver's license and license number and terms such as UT or Utah.

Driver's license pattern: 6 - 10 Numeric

Virginia License Number Content Blade

The content blade looks for matches to the Virginia driver's license pattern and words and phrases such as driver's license and license number and terms such as VA or Virginia.

Driver's license pattern: 1 Alphabetic, 8 Numeric

Visa Card Number Content Blade

The content blade looks for a combination of the following pieces of information, either:

1 More than one JCB credit card number

2 A single credit card number plus words and phrases such as ccn, credit card, expiration date

3 A single credit card number plus an expiration date

Washington License Number Content Blade

The content blade looks for matches to the Washington driver's license pattern and words and phrases such as driver's license and license number and terms such as WA or Washington.

Driver's license pattern: 5 Alphabetic (last name), 1 Alphabetic (first name), 1 Alphabetic (middle name), 3 Numeric, 2 Alphanumeric. If last or middle name field falls short, fill with *s.

Wisconsin License Number Content Blade

The content blade looks for matches to the Wisconsin driver's license pattern and words and phrases such as driver's license and license number and terms such as WI or Wisconsin.

Driver's license pattern: 1 Alphabetic, 13 Numeric

Wyoming License Number Content Blade

The content blade looks for matches to the Wyoming driver's license pattern and words and phrases such as driver's license and license number and terms such as WY or Wyoming.

Driver's license pattern: 9 - 10 Numeric

File Formats Supported by Data Security

18

NSX Data Security can detect the following file formats.

Table 18-1. Archive Formats

Application Format	Extensions
7-Zip 4.57	7Z
BinHex	HQX
BZIP2	BZ2
Expert Witness (EnCase)Compression Format	E0, E101 etc
GZIP 2	GZ
ISO-9660 CD Disc Image Format	ISO
Java Archive	JAR
Legato EMailXtender Archive	EMX
MacBinary	BIN
Mac Disk copy Disk Image	DMG
Microsoft Backup File	BKF
Microsoft Cabinet Format 1.3	CAB
Microsoft Compressed Folder	LZH LHA
Microsoft Entourage	
Microsoft Outlook Express	DBX
Microsoft Outlook Offline Store 2007	OST
Microsoft Outlook Personal Store 2007	PST
OASIS Open Document Forma	ODC SXC STC ODT SXW STW
Open eBook Publication Structure	EPUB
PKZIP	ZIP
RAR archive	RAR
Self-extracting Archives	SEA

Table 18-1. Archive Formats (Continued)

Application Format	Extensions
Shell Scrap Object File	SHS
Tape Archive	TAR
UNIX Compress	Z
UUEncoding	UUE
WinZip	ZIP

Table 18-2. Computer-Aided Design Formats

Application Format	Extensions
CATIA formats 5	CAT
Microsoft Visio 5, 2000, 2002, 2003, 2007	VSD
MicroStation 7, 8	DGN
Omni Graffle	GRAFFLE

Table 18-3. Database Formats

Application Format	Extensions
Microsoft Access 95, 97, 2000, 2002, 2003, 2007	MDB

Table 18-4. Display Formats

Application Format	Extensions
Adobe PDF 1.1 to 1.7	PDF

Table 18-5. Mail Formats

Application Format	Extensions
Domino XML Language	DXL
Legato Extender	ONM
Lotus Notes database 4, 5, 6.0, 6.5, 7.0, and 8.0	NSF
Mailbox Thunderbird 1.0 and Eudora 6.2	MBX
Microsoft Outlook 97, 2000, 2002, 2003, and 2007	MSG
Microsoft Outlook Express Windows 6 and MacIntosh 5	EML
Microsoft Outlook Personal Folder 97, 2000, 2002, and 2003	PST
Text Mail (MIME)	Various

Table 18-6. Multimedia Formats

Application Format	Extensions
Advanced Streaming Format 1.2	DXL

Table 18-7. Presentation Formats

Application Format	Extensions
Apple iWork Keynote 2, 3, ‘08, and ‘09	GZ
Applix Presents 4.0, 4.2, 4.3, 4.4	AG

Table 18-7. Presentation Formats (Continued)

Application Format	Extensions
Corel Presentations 6, 7, 8, 9, 10, 11, 12, and X3	SHW
Lotus Freelance Graphics 2	PRE
Lotus Freelance Graphics 96, 97, 98, R9, and 9.8	PRZ
Macromedia Flash through 8.0	SWF
Microsoft PowerPoint PC 4	PPT
Microsoft PowerPoint Windows 95, 97, 2000, 2002, and 2003	PPT, PPS, POT
Microsoft PowerPoint Windows XML 2007	PPTX, PPTM, POTX, POTM, PPSX, and PPSM
Microsoft PowerPoint Macintosh 98, 2001, v.X, and 2004	PPT
OpenOffice Impress 1 and 1.1	SXP
StarOffice Impress 6 and 7	SXP

Table 18-8. Spreadsheet Formats

Application Format	Extensions
Apple iWork Numbers '08 and 2009	GZ
Applix Spreadsheets 4.2, 4.3, and 4.4	AS
Comma Separated Values	CSV
Corel Quattro Pro 5, 6, 7, 8, X4	WB2. WB3, QPW
Data Interchange Format	DIF
Lotus 1-2-3 96, 97, R9, 9.8, 2, 3, 4, 5	123, WK4
Lotus 1-2-3 Charts 2, 3, 4, 5	123
Microsoft Excel Windows 2.2 through 2003	XLS, XLW, XLT, XLA
Microsoft Excel Windows XML 2007	XLSX, XLTX, XLSM, XLTM, XLAM
Microsoft Excel Charts 2, 3, 4, 5, 6, 7	XLS
Microsoft Excel Macintosh 98, 2001, v.X, 2004	XLS
Microsoft Office Excel Binary Format 2007	XLSB
Microsoft Works Spreadsheet 2, 3, 4	S30 S40
Oasis Open Document Format 1, 2	ODS, SXC, STC
OpenOffice Calc 1, 1.1	SXC, ODS, OTS
StarOffice Calc 6, 7	

Table 18-9. Text and Markup Formats

Application Format	Extensions
ANSI	TXT
ASCII	TXT
Extensible Forms Description Language	XFDL, XFD
HTML 3, 4	HTM, HTML
Microsoft Excel Windows XML 2003	XML
Microsoft Word Windows XML 2003	XML
Microsoft Visio XML 2003	vdx

Table 18-9. Text and Markup Formats (Continued)

Application Format	Extensions
MIME HTML	MHT
Rich Text Format 1 through 1.7	RTF
Unicode Text 3, 4	TXT
XHTML 1.0	HTM, HTML
XML (generic)	XML

Table 18-10. Word Processing Formats

Application Format	Extensions
Adobe FrameMaker InterchangeFormat 5, 5.5, 6, 7	MIF
Apple iChat Log AV, AV 2, AV 2.1,AV 3	LOG
Apple iWork Pages '08, 2009	GZ
Applix Words 3.11, 4, 4.1, 4.2, 4.3,4.4	AW
Corel WordPerfect Linux 6.0, 8.1	WPS
Corel WordPerfect Macintosh 1.02, 2, 2.1, 2.2, 3, 3.1	WPS
Corel WordPerfect Windows 5, 5.1, 6, 7, 8, 9, 10, 11, 12, X3	WO, WPD
DisplayWrite 4	IP
Folio Flat File 3.1	FFF
Founder Chinese E-paper Basic 3.2.1	CEB
Fujitsu Oasys 7	OA2
Haansoft Hangul 97, 2002, 2005, 2007	HWP
IBM DCA/RFT (Revisable Form Text) SC23-0758 -1	DC
JustSystems Ichitaro 8 through 2009	JTD
Lotus AMI Pro 2, 3	SAM
Lotus AMI Professional Write Plus 2.1	AMI
Lotus Word Pro	96, 97, R9
Lotus SmartMaster 96, 97	MWP
Microsoft Word PC 4, 5, 5.5, 6	DOC
Microsoft Word Windows 1.0 and 2.0, 6, 7, 8, 95, 97, 2000, 2002, 2003	DOC
Microsoft Word Windows XML 2007	DOCX, DOTX, DOTM
Microsoft Word Macintosh 4, 5, 6, 98, 2001, v.X, 2004	DOC
Microsoft Works 2, 3, 4, 6, 2000	WPS
Microsoft Windows Write 1, 2, 3	WRI
Oasis Open Document Format 1, 2	ODT, SXW, STW
OpenOffice Writer 1, 1.1	SXW, ODT
Omni Outliner 3	OPML, OO3, OPML, OOUTLINE
Skype Log File	DBB
StarOffice Writer 6, 7	SXW, ODT
WordPad through 2003	RTF

Table 18-10. Word Processing Formats (Continued)

Application Format	Extensions
XML Paper Specification	XPS
XyWrite 4.12	XY4

Index

A

activity monitoring
- about **186**
- AD groups that accessed a server **194**
- disable **195**
- enable data collection for multiple VMs **189**
- enable data collection for single VM **189**
- inbound activity **190**
- interaction between inventory containers **193**
- outbound activity **191**
- virtual machine activity **190**

add, service **154**
alarms for Guest Introspection **196**
appliance
- add **169**
- delete **170**
- edit **169**

Audit Logs **152, 160**
audit messages for Guest Introspection **197**

B

backups **178**

C

content blades
- ABA Routing Number **236, 260**
- Admittance and Discharge Dates Content Blade **236, 260**
- Alabama Drivers License Content Blade **236, 260**
- Alaska Drivers License Content Blade **236, 237, 261**
- Alberta Drivers Licence Content Blade **237, 261**
- American Express Content Blade **237, 261**
- Arizona Drivers License Content Blade **237, 261**
- Arkansas Drivers License Content Blade **236, 237, 257, 262**
- Australia Bank Account Number Content Blade **238, 262**
- Australia Business Number Content Blade **238, 262**
- Australia Company Number Content Blade **238, 262**
- Australia Medicare Card Number Content Blade **238, 262**
- Australia Tax File Number Content Blade **238, 262**
- California Drivers License Number Content Blade **238, 263**
- Canada Drivers License Number Content Blade **239, 263**
- Canada Social Insurance Number Content Blade **239, 263**
- Colorado Drivers License Number Content Blade **239, 263**
- Connecticut Drivers License Number Content Blade **239, 263**
- Credit Card Track Data Content Blade **239, 263**
- Custom Account Number Content Blade **240, 264**
- Delaware Drivers License Number Content Blade **240, 264**
- EU Debit Card Number Content Blade **240, 264**
- Florida Drivers License Number Content Blade **240, 264**
- France BIC Number Content Blade **240, 264**
- France Driving License Number Content Blade **240, 264**
- France National Identification Number Content Blade **241, 265**
- France VAT Number Content Blade **241, 265**
- Georgia Drivers License Number Content Blade **241, 265**
- Germany Driving License Number Content Blade **241, 265**
- Germany BIC Number Content Blade **241, 265**
- Germany National Identification Numbers Content Blade **241, 265**
- Germany Passport Number Content Blade **242, 266**
- Germany VAT Number Content Blade **242, 266**
- Group Insurance Numbers Content Blade **242, 266**
- Hawaii Drivers License Number Content Blade **242, 266**

Idaho Drivers License Number Content Blade **243, 267**
Illinois Drivers License Number Content Blade **243, 267**
Index of Procedures Content Blade **243, 267**
Indiana Drivers License Number Content Blade **243, 267**
Iowa Drivers License Number Content Blade **243, 267**
Italy Driving License Number Content Blade **244, 268**
Italy IBAN Number Content Blade **244, 268**
Italy National Identification Numbers Content Blade **242, 266**
ITIN Unformatted Content Blade **244, 268**
Kansas Drivers License Number Content Blade **245, 269**
Kentucky Drivers License Number Content Blade **245, 269**
Louisiana Drivers License Number Content Blade **245, 269**
Maine Drivers License Number Content Blade **245, 269**
Manitoba Drivers Licence Content Blade **245, 269**
Maryland Drivers License Number Content Blade **246, 270**
Michigan Drivers License Number Content Blade **246, 270**
Minnesota Drivers License Number Content Blade **246, 270**
Mississippi Drivers License Number Content Blade **246, 270**
Missouri Drivers License Number Content Blade **246, 270**
Montana Drivers License Number Content Blade **246, 270**
NDC Formulas Dictionary Content Blade **246, 270**
Nebraska Drivers License Number Content Blade **247, 271**
Netherlands Driving Licence Number Content Blade **247, 271**
Netherlands IBAN Number Content Blade **247, 271**
Netherlands National Identification Numbers Content Blade **247, 271**
Netherlands Passport Number Content Blade **248, 272**
New Brunswick Drivers Licence Content Blade **248, 272**
New Hampshire Drivers License Number Content Blade **248, 272**
New Jersey Drivers License Number Content Blade **248, 272**
New Mexico Drivers License Number Content Blade **248, 272**
New York Drivers License Number Content Blade **248, 272**
New Zealand Health Practitioner Index Number Content Blade **249, 273**
New Zealand Inland Revenue Department Number **249, 273**
New Zealand National Health Index Number Content Blade **249, 273**
Newfoundland and Labrador Drivers Licence Content Blade **249, 273**
North Carolina Drivers License Number Content Blade **249, 273**
North Dakota Drivers License Number Content Blade **249, 273**
Nova Scotia Drivers Licence Content Blade **249, 273**
Ohio Drivers License Number Content Blade **249, 273**
Oklahoma License Number Content Blade **250, 274**
Ontario Drivers Licence Content Blade **250, 274**
Oregon License Number Content Blade **250, 274**
Patient Identification Numbers Content Blade **250, 274**
Pennsylvania License Number Content Blade **250, 274**
Prince Edward Island Drivers Licence Content Blade **250, 274**
Protected Health Information Terms Content Blade **250, 274**
Quebec Drivers Licence Content Blade **251, 275**
Rhode Island License Number Content Blade **251, 275**
Saskatchewan Drivers Licence Content Blade **251, 275**
SIN Formatted Content Blade **251, 275**
SIN Unformatted Content Blade **251, 275**
South Carolina License Number Content Blade **252, 276**
South Dakota License Number Content Blade **252, 276**
Spain National Identification Number Content Blade **252, 276**
Spain Passport Number Content Blade **252, 276**
Spain Social Security Number Content Blade **252, 276**
SSN Formatted Content Blade **251, 275**
SSN Unformatted Content Blade **252, 276**

Sweden IBAN Number Content Blade **252, 276**
Sweden Passport Number Content Blade **253, 277**
Tennessee License Number Content Blade **253, 277**
UK Driving License Number Content Blade **253, 277**
UK IBAN Number Content Blade **254, 278**
UK NINO Formal Content Blade **254, 278**
UK Passport Number Content Blade **254, 278**
Utah License Number Content Blade **255, 279**
Virginia License Number Content Blade **255, 279**
Visa Card Number Content Blade **255, 279**
Washington License Number Content Blade **255, 279**
Wisconsin License Number Content Blade **255, 279**
Wyoming License Number Content Blade **255, 279**

D

Data Security,policy,regulations **135**
Data Security,user roles **135**
date **161**
DHCP **110**
DHCP relay
about **112**
add agents **113**
add server **113**
domain **164, 165**

E

events, syslog format **160**
events for Guest Introspection **197**

F

firewall
add rule **43**
add section **50**
change rule order **49**
CPU and memory thresholds **56**
delete rule **50**
exclude virtual machines **52**
export configuration **51**
import configuration **51**
load configuration **52**
merge sections **50**
selete section **51**
flow monitoring
date range **184**
IPFix **179**
live flows **185**
Flow Monitoring
enable **179**
exclude flows **179**
firewall rules **185**
flow monitoring data **182**

G

Guest Introspection
alarms **196**
audit messages **197**
events **197**
host alarms **196**
status **196**
SVM alarms **197**
GUI, logging in **161**

H

high availability **175**
host alarms for Guest Introspection **196**

I

introduction, NSX **14**
IPSec VPNS **86**
IPSec service
delete **89**
disable **89**
IPSec VPN
add **87**
configuration examples **199**
edit **88**
enable **86**
global configuration **86**
logging **87**
overview **85**

L

L2 VPN
client **93**
enable **93**
overview **89**
server **92**
statistics **95**
L2 bridge **31, 32**
live traffic flows **185**
load balancer, add pool **99**
logging in to the GUI **161**
logical network **21, 24**
logical switch
about **19**
add **21**
connect to NSX Edge **22**
connect VMs to **23**
deploy services on **23**

edit **24**
ping test **23**
prevent spoofing on **24**
scenario **26**
logs, audit **152, 160**

M

Massachusetts Drivers License Number Content Blade **246, 270**

N

NAT **61**
NSX
consumption platform **15**
control plane **15**
data plane **15**
management plane **15**
overview **13**
services **16**
NSX Data Security
about **135**
policy **135**
scan **137**
supported file formats **281**
user roles **135**
NSX Edge
add appliance **169**
add NAT rules **61**
certificate revocation list **168**
certificates **166**
client certificates **168**
configure CA signed certificate **166**
configure self signed certificate **167**
delete appliance **170**
DHCP **109**
DHCP binding **111**
DHCP pool add **109**
DNS servers **113**
edit appliance **169**
firewall rules
add **57**
change priority **60**
delete **61**
edit **60**
force sync **176**
interface
delete **171**
disable **172**
nterface, enable **171**
SSL VPN overview **65**
status **176**
syslog **176**
NSX Edge firewall rules, change default settings **57**
NSX Edge interface **170**
NSX Edge, DHCP binding edit **112**
NSX Edge, DHCP pool edit **110**
NSX Manager
backups **178**
DNS servers **162**
events **160**
import certificate **164**
logging in to GUI **161**
lookup service **162**
NTP server **161**
restore a backup **179**
SSL certificate **163**
syslog server **161**
vCenter Server **162**
NSX ticket logger **159**

R

redeploy NSX Edge **177**
regulations
ABA Routing Numbers **221**
Arizona SB-1338 **221**
Australia Bank Account Numbers **221**
Australia Medicare Card Numbers **222**
Australia Tax File Numbers **222**
California AB-1298 **222**
California SB-1386 **223**
Canada Drivers License Numbers **223**
Canada Social Insurance Numbers **223**
Colorado HB-1119 **224**
Connecticut SB-650 **224**
Credit Card Numbers **224**
Custom Account Numbers **224**
EU Debit Card Numbers **225**
FERPA (Family Educational Rights and Privacy Act) **225**
Florida HB-481 **225**
France IBAN Numbers Policy **225**
France National Identification Numbers Policy **225**
Georgia SB-230 Policy **226**
Germany BIC Numbers Policy **226**
Germany Driving License Numbers Policy **226**
Germany IBAN Numbers Policy **226**
Germany National Identification Numbers Policy **226**
Germany VAT Numbers Policy **226**
Hawaii SB-2290 Policy **227**
HIPPA (Healthcare Insurance Portability and Accountability Act) Policy **227**

Idaho SB-1374 Policy **227**
Illinois SB-1633 **228**
Indiana HB-1101 Policy **228**
Italy Driving License Numbers Policy **228**
Italy IBAN Numbers Policy **228**
Italy National Identification Numbers Policy **228**
Kansas SB-196 Policy **229**
Louisiana SB-205 Policy **229**
Maine LD-1671 Policy **229**
Massachusetts CMR-201 **230**
Minnesota HF-2121 **230**
Montana HB-732 Policy **230**
Netherlands Driving Licence Numbers **230**
Nevada SB-347 **231**
New Hampshire HB-1660 **231**
New Jersey A-4001 **231**
New York AB-4254 **232**
New Zealand Inland Revenue Department Numbers **232**
New Zealand Ministry of Health Numbers **232**
Ohio HB-104 **232**
Oklahoma HB-2357 **233**
Patient Identification Numbers **233**
Payment Card Industry Data Security Standard (PCI-DSS) **233**
Texas SB-122 **233**
UK BIC Numbers **234**
UK Driving Licence Numbers **234**
UK IBAN Numbers **234**
UK National Health Service Numbers **234**
UK National Insurance Numbers (NINO) **234**
UK Passport Numbers **234**
US Drivers License Numbers Policy **235**
US Social Security Numbers **235**
Utah SB-69 **235**
Vermont SB-284 **235**
Washington SB-6043 **236**
reports, audit log **152, 160**
restore a backup **179**

S

security groups, add **152**
security policy
create **119**
delete **130**
edit **129**
manage priority **129**
map to security group **122**
view effective services **128**
security group
create in Service Composer **117**
edit in Service Composer **130**
server pool
delete **106**
edit **106**
service, add **154**
Service Composer
about **116**
canvas view **122**
export configuration **125**
import configuration **125**
scenarios **130**
security group
create **117**
edit **130**
security policy
delete **130**
edit **129**
manage priority **129**
map to security group **122**
view effective services **128**
view effective services on VM **128**
view service failures **128**
security tag
add **126**
assign **127**
delete **127**
edit **127**
view **126**
security policy create **119**
single sign on **143**
spoofGuard
about **53**
approve IP address **54**
create policy **53**
edit IP address **54**
system policy **53**
spoofGuard. clear IP address **55**
SSL VPN-plus, authentication, add **68, 75**
SSL VPN
client configuration **79**
edit general settings **80**
edit portal design **80**
login/logoff script
add **73, 79**
delete **84**
disable **85**
edit **84**
enable **85**
login/logoff scripts, change the order of **85**
logs **79**
web resource **74**

SSL VPN-Plu, IP pool, change order of **81**
SSL VPN-Plus
  add installation package **71**
  add IP pool **67**
  add private network **67**
  add user **72, 74**
  enable **72, 78**
    installation package
      add **71**
      delete **83**
    IP pool
      add **67**
      delete **81**
      disable **81**
      edit **81, 152**
    private network
      change order of **82**
      delete **82**
    users
      add **72, 74**
      change password **84**
      delete **84**
      edit **83**
SSL VPN,overview **65**
static route, add **34**
status
  Guest Introspection **196**
  NSX Edge **176**
supported file formats **281**
SVM alarms for Guest Introspection **197**
syslog, NSX Edge **176**
syslog server **161**
syslog format **160**
system events **159**

T

technical support logs
  NSX Edge **177**
  NSX Manager **163**
test **100**
transport zone **21, 24–26**

U

upgrade, NSX Edge **177**
user account
  about user roles **144**
  assign role to **145**
  change role **148**
  delete **148**
  disable **148**
  edit **147**
  enable **148**
  manage default account **145**
  single sign on **143**

V

vCenter Server, change for NSX Manager **162**
view, VM activity **190**
virtual server
  delete **107**
  edit **106**
virtual wire, create **20**
VPN, configure service **87**
vShield Edge, HA **175**