Forcepoint NGFW Study Guide

December 4, 2018

Contents

PART I

INFRASTRUCTURE

Chapter 1

The SMC - Security Management Center

1.1 Summary

In this chapter, you will learn about the system architecture and learn the architectural overview of the SMC. This chapter will introduce you to the NGFW and the SMC, or Security Management Center. The goal is to familiarize you with the basic capabilities of the NGFW and SMC and how they fit together to form a firewall infrastructure. At the end of this chapter, you will understand how to select the correct NGFW deployment and size the SMC accordingly.

1.2 Key Concepts

1. NGFW System Architecture
   - Sizing and Capacity
   - Installation and Upgrade
2. SMC Architecture and Overview
   - Sizing and Capacity
3. Management Server High Availability
4. Log Server High Availability
5. SMC Updates
6. Licensing Model

1.3 Concepts In Detail

1.3.1 NGFW System Architecture

- The NGFW has **three** operating roles:
  1. **Firewall/VPN**: full layer 3 firewall capable of static routing, dynamic routing, IPSec VPN formation and termination, full deep inspection, and, when used in a multi-layer deployment, it can also be configured with Layer 2 interfaces. The default firewall action is **discard**.
  2. **Layer 2 Firewall**: operates at layer 2 and, as such, there is no routing or IPSec VPN. Designed to be used in networks where segmentation is needed but topology changes to the network are unwanted (introducing NAT requires network topology changes). It is capable of full deep inspection. Like the Firewall/VPN, the default action is discard.

3. **IPS**: operates as a layer 2 device. The primary function of the IPS role is as a dedicated device to perform deep inspection on network traffic flowing through it, identify attacks, and prevent evasions (hacking techniques designed to bypass a firewall).

NGFW Engine Appliance

1. Runs a hardened version of Linux, custom designed by Forcepoint and is purpose-built for security.

2. Any patches or fixes are part of an engine upgrade. Upgrades can be performed “over the wire“ from the SMC.

3. There are desktop model appliances (e.g. NGFW 110 and 115) all the way up to the datacenter (e.g. NGFW 6205). Each of these has their own characteristics for performance and throughput. Please refer to the Student Guide for more detail.

4. The NGFW solution is software. Because of that, the NGFW can be run on a variety of platforms:

   - Appliance
   - Virtual Machine (VMWare, KVM, Oracle)
   - AWS
   - Microsoft Azure
   - Virtual Context (see below)

Installation Methods

Each firewall has to be deployed, and they must communicate with the SMC to establish a trust relationship using certificates. The following methods are available:

1. USB installation method

2. Manual installation method

3. Cloud installation method

Please refer to the Student Guide for additional detail.

1.3.2 SMC Architecture Overview

- The SMC (Security Management Center) is the central point of administration for all NGFWs - regardless of role or location.

- The SMC can manage NGFWs, regardless of location.

- There are three (3) components that form the SMC:

  1. **Management Server**: this is the central repository for all information about the system. The Management server has a database where all policies and network objects are stored. It communicates with the engines to send commands and install security policies. All management of the NGFW is driven through the Management and Log servers. There is no direct access from the Management Client to the NGFW - all actions are driven through the SMC.
  2. **Log Server**: this receives all logs and health information from the engines. Monitoring of the entire system, management and NGFW, is performed by the log server.
  3. **Web Portal Server**: this is an optional component that provides read-only access to logs, reports, and policies (via HTML). This is used in cases where read-only access to logs, reports, and policies is required while not defining them as an SMC administrator.

1.3.3 Management Server High Availability

The SMC supports high availability in Active/Standby mode. This feature is intended primarily for disaster recovery purposes. The following are the key features:

1. There can be a total of 5 management servers, one active, and four in stand-by mode.
2. Replication of data from the active management servers to the stand-by servers is **incremental**.
3. You can control all management servers from the Management Client, allowing you to manually synchronize data between SMCs, activate a management server or put it standby mode.
4. The selection of an active management server is manual - failover is not automatic, allowing the administrator full control over which management server is best suited to take over.
5. To create a stand-by management server, perform the SMC installation in the usual manner, except you select your new management server as a stand-by server for your primary SMC.
6. A special license is needed for the SMC HA feature.

1.3.4 Log Server High Availability

1. Allows one log server to act as the backup for another log server.
2. Engines are configured to use one log server as the primary and the other as backup. Should the primary fail or become unavailable, the NGFW begins logging to the backup automatically.
3. There is no synchronization between log servers.
4. There is no special license required for Log Server HA.

1.3.5 Upgrading the SMC

Upgrading the SMC is as simple as running the installer for the new version. The installation detects the current version and upgrades it. For non-HA installations, the management server and log server are stopped and upgraded. For HA installations, the primary is upgraded first and the then the stand-by servers. For additional, detailed information, please refer to the Student Guide. All servers in the SMC (Management, Log, and Web Portal) must be at the same software version. At a high level, the following steps are required:

1. Upgrade the licenses
2. Upgrade all SMC components
3. Upgrade the NGFWs

1.3.6 Management and NGFW Licensing

Please refer to the Student Guide for detailed information, but the following information will be helpful during the exam:

1. Each component requires a license of its own, e.g. Management Server license, Log Server license, NGFW license.
2. The Management Server license is bound to its IP address
3. Each managed entity consumes one SMC license count. For example, if you have an SMC-10 license, allowing you to manage 10 things, then if you manage a single NGFW, you would have 9 SMC licenses left. However, from the perspective of the SMC, a firewall cluster is considered one managed entity, and therefore only consumes one SMC license count, regardless of the number of nodes in the cluster.
4. Monitoring a third-party device consumes .2 SMC licenses.

1.4 Review

Remember the following:

1. The same appliance can be used for any role.
2. All roles have the same level of deep inspection capabilities.
3. All roles provide protection against evasions.
4. Most of the security features are available in all roles. Infrastructure features such as Multi-Link, dynamic routing, IPSec VPNs, etc. are only available in the Firewall/VPN role.
5. Forcepoint Cloud integrations are available in all roles, e.g. Web Filtering, Anti-Malware, and Advanced Malware Detection.
6. Each appliance can be run in one of the three operating roles, firewall/VPN, layer 2 firewall, or IPS.
7. Each appliance comes licensed to run a certain number of **virtual contexts**. A virtual context is one or more logical instances of the NGFW running on the same NGFW appliance. This is not virtualization in the strictest since, as there is no hypervisor. This allows you to run several firewall instances on the same appliance, which is a benefit for those looking to utilize the hardware fully or for MSSPs.
8. When an appliance is running virtual contexts (logical instances of the NGFW running on the same appliance), it is referred to as a **Master Engine**.
9. The Firewall/VPN role needs at least **two** interfaces, one for outbound network traffic and SMC communication, and the other for internal networks.
10. The IPS role (when used as an in-line IPS) needs 3 interfaces, one for SMC communication and two for traffic to come in and go out.
11. The Layer 2 Firewall role requires at least 3 interfaces, one for SMC communication and two for controlling traffic.
12. The primary way of upgrading NGFWs is via the Management Client, “over the wire“.
13. The Management, Log, and Web Portal servers can be installed on the same machine or physically separate machines.
14. The SMC servers can be installed as virtual machines.
15. The SMC will run on Linux (usually CentOS 7 and later) and on Windows Server versions, Server 2012 and later.
16. The Log Server can process more than 100,000 records per second.
17. The Management server can manage up to 2000 NGFW.
18. The number of stand-by Management Servers.
19. License requirements for Log and Management Server HA.
20. Apart from Forcepoint integrations (Web Filtering, Forcepoint Advanced Malware Detection, etc.), all NGFW features are part of the base license.
21. The fail-over method for Management Server HA.
22. The number of stand-by Log Servers (one).
23. The SMC Client can be installed locally on your computer or deployed via Java Webstart from the SMC.

Chapter 2

Single Firewall Deployment and Routing

2.1 Summary

This section deals with the Firewall/VPN role and deploying a Single Firewall. This section looks at the key features and benefits of the NGFW, and how to deploy a single (i.e. non-clustered) NGFW.

2.2 Key Concepts

1. NGFW Capabilities and Key Features
2. Single Firewall Overview
3. Additional Firewall Features

2.3 NGFW Capabilities and Key Features

The features of the NGFW can be broken down into two main categories, infrastructure and security. Below is a list of key features to keep in mind:

1. **Infrastructure**:
    - Multi-Link (ISP Load Balancing)
    - VPN (and Multi-Link VPN)
    - Clustering. Up to 16 nodes can be clustered together.
    - Centralized Management
    - A single NGFW software package that allows you to run the NGFW as a Firewall/VPN, a Layer 2 firewall, or an IPS.
2. **Security**
    (a) Multi-layer inspection of network traffic
    (b) Full IPS (deep inspection) capabilities are available in all roles
    (c) Evasion detection available in all roles.
    (d) Forcepoint Integrations - Web Filtering, Anti-Malware, and Cloud Sandboxing (Forcepoint Advanced Malware Detection)

The NGFW uses a multi-layer inspection technique that consists of the following:

- Packet Filtering

- Stateful Inspection
- Application Layer deep inspection
- Protocol Agents (explained in more detail later)
- Application Identification
- Deep Inspection (IPS capabilities)
- Forcepoint Cloud Services
- Evasion Detection and Prevention

2.4 Single Firewall Deployment

A single firewall installation is one in which clustering is not involved. As a single firewall, there are some features that are supported that are not supported in a clustered installation:

1. Dynamic interfaces (ADSL). In the case of a dynamic interface, *the NGFW will contact the management server periodically for any commands*
2. Wireless interfaces

NOTE: Make sure to review the student guide on the steps for defining a single firewall.

When defining a firewall, you must define interfaces for the firewall. Each of those interfaces has a specific function, or interface option. Make sure to understand the following interface options:

1. Control Interface Primary
2. Control Interface Backup
3. Identity for Authentication Requests
4. Source for Authentication Requests
5. Default IP Address for Outgoing Traffic

2.5 Additional NGFW Features

In addition to the basic features of the NGFW covered in this and previous modules, there are some additional features available.

1. Interfaces can be normal, which is the default, or they can be:
   - Aggregated Link for High Availability. This uses LACP to bond the interfaces so that should one interface go down, there is another one left.
   - Aggregated Link for Load Balancing. This allows packets to be balanced between interfaces. Both of these interface types require that the switch to which they connect supports LACP.
2. DHCP Server. This will assign addresses to hosts behind the firewall. It will not assign addresses to Mobile VPN users.
3. DNS Relay. This will relay DNS requests to an external DNS server. It reduces load on upstream DNS servers, improves DNS performance, and allows fixed DNS results for specific hosts or domains.

2.6 Routing and Anti-spoofing

The NGFW is capable of two main types of routing:

1. **Static**: In Static routing, the Routing view in the NGFW properties is used to create the routing table. There are two ways to add routes: one is to add them using a visual, menu-driven approach, the other is typing the routes into the routing editor. Static routes define a path to a network resource.

2. **Dynamic**: In dynamic routing, routes a created based on several protocols supported by the NGFW. These include BGP, OSPF, and RIP. Adjusting the anti-spoofing my be necessary.

There are extensions to these concepts. These include:

1. **Static Multicast Routing**: The NGFW can forward multicast frames using several different protocols. These include PIM-SM, PIM-DM, and PIM-SSM. The NGFW can also act as an IGMP proxy. Please refer to the Student Guide for additional details.

2. **Policy-Based Routing**: Policy-based routing are entries that are processed before the routing table that will send packets to a destination they might not otherwise go according to the routing table. Policy-based routing may require changes to anti-spoofing. Please see the Student Guide for additional detail.

Anti-spoofing is essentially the process of ensuring that packets are arriving on the correct interface. Anti-spoofing has the following characteristics:

1. Anti-spoofing is based on the routing table. Generally speaking, if the routing table is correct, then the anti-spoofing is also correct.

2. Anti-spoofing is one of the very first checks the firewall performs when processing packets, and it ensures that packets arrive on the intended interface. This prevents attackers from spoofing an IP on the internal network, for example.

Remember the following:

1. Review the key features of the NGFW.

2. The NGFW license enables all major features of the NGFW, apart from cloud-based services such as URL Filtering (ThreatSeeker), Anti-Malware, and Advanced Malware Detection (both cloud and on-premise).

3. Review the parts of multi-layer inspection.

4. To define an NGFW, you must define the firewall, give it a name and select a log server, define physical interfaces first, add IP addresses to those interfaces, and ensure that the routing is correct. The last step is to save the initial configuration, which is used to establish trust with the SMC. With the initial configuration, contact with the SMC can be done manually (using the NGFW command line), with a USB stick, or the Cloud installation method.

5. If the initial configuration of the engine is done manually, at the command line, you must supply the IP address of the engine, subnet mask, default gateway, the IP of the management server and the One-Time password that is found in the initial configuration file.

6. Every NGFW, regardless of role, must have one management interface. The minimum required number of interfaces for the Firewall/VPN role is 2, 3 for an in-line IPS, 2 for an IPS in listen-only mode (IDS), and 3 for the Layer 2 firewall.

7. Know the difference between the interface options “Source for Authentication Requests“ and “Identity for Authentication Requests“.

8. Refer to the Student Guide and review the NGFW Add-Ons and understand the role of the “Advanced“ options in the NGFW properties.

9. Static routing is manually defined using the Management Client. The routing view can be found in the firewall properties.

10. Dynamic routing is supported - BGP, OSPF, and RIP. RIP is one of the only things configured at the command line of the engine. BGP and OSPF are configured through the Management Client.

11. Policy-Based routing sends packets from a particular network via some other path and superceeds the routing table.

12. Anti-spoofing is one of the first checks the firewall performs, and is generated automatically based on the routing table. This prevents IP spoofing attacks.

Chapter 3

Policy Templates, Access Rules and NAT

3.1 Summary

This chapter covers concepts related to NGFW policies. NGFW policies define the rules that would would like to enforce for controlling network traffic. There are several approaches to defining rules, and there are many object types that can be used, allowing for very detailed control of network traffic.

3.2 Key Concepts

- Policy Types
- Firewall Templates and Policy Structure
- Special Objects and Actions
- The Anatomy of the Policy Editor
- Options for Rules
- Policy Installation and Activation

3.3 Policy Types

Each role has it's own policy type. The following are the policy types:

1. Firewall Policy
2. Layer 2 Firewall Policy
3. IPS Policy

These policies allow you to configure rules for each role. Each of these policies have their own access rules. In any Layer 2 policy, such as the Layer 2 firewall and IPS, there will also be ethernet access rules, allowing you to control layer 2 protocols.

There are types of rules that are found in each policy. Below is a list of rule types that are present in each policy type:

1. **Firewall Policy**
    - Access Rules
    - NAT Rules
    - Inspection Rules (optional)

- File Filtering Rules (optional)
- Layer 2 Interface Policy (optional). These rules would only be applicable in Layer 2 interfaces were defined. Please refer to the Student Guide for more detail.

2. **Layer 2 Firewall Policy**
   - Ethernet Access Rules
   - IPv4/IPv6 Access Rules
   - Inspection Rules (optional)
   - File Filtering Rules (optional)
3. **IPS**
   - Ethernet Access Rules
   - IPv4/IPv6 Access Rules
   - Inspection Rules
   - File Filtering Rules (optional)

NOTE: Inspection rules and file filtering rules exist as their own collection of rules (or policy) that is associated with the main policy. For example, if you are using the NGFW in the Firewall/VPN role, you can define an Inspection Policy that is then associated with the Firewall policy in the Inspection tab of the policy editor. This is far more organized way to manage policies.

3.4 Firewall Templates and Policy Structure

Every policy type that you can define has a template, defined by Forcepoint, upon which you will base all policies that you define. These templates contain, among other things:

- Rules that allow communication from the SMC to the NGFW and back
- Rules the define how the NGFW handles particular protocols
- Rules that define which protocols are being sent for deep inspection

The rules contained in the template are processed before your custom defined rules. Most of the templates are not visible from the policy editor. These “automatic rules“ are designed by Forcepoint and not meant to be edited. A summary of these can be viewed in the NGFW properties. These policy templates cannot be edited.

In addition to these pre-defined templates, you can also create your own templates. These templates can be used by more than one NGFW. Templates are designed to better organize rule bases, reduce the chance of error, and enable greater agility when making policy changes that effect all firewalls under management. Please refer to the Student Guide for additional information.

To speed up the processing of the policy rules, sub-policies can be used. These allow you to group rules together that have something in common. For example, if you had 20 rules that all had to do with things in the DMZ, you could create a rule that said, “if the source is not my internal networks, and the destination is the DMZ, jump to the DMZ sub-policy. The sub-policy itself is a separate collection of rules. If the “jump“ rule does not match, referencing the sub-policy, then the firewall can skip over them, thereby increasing the processing speed.

3.5 Special Objects

In order for a template, which used by many firewalls, to be general enough to be used on multiple firewalls - all with different configurations - special objects are used to accomplish this:

1. Alias objects

2. Expressions. Although not specifically covered in the Student Guide, this is designed to narrow the scope of a source or destination. For example, you would like to define the "Internet" as being things that are not your internal networks. Expressions allow you to use operators such as NOT, Union, Intersect, etc. These are used extensively in the System Engineer Course labs.
3. Continue Rules

Please refer to the Student Guide for detailed information on these concepts. Continue rules are most often used in templates. Continue Rules allow you to define the following:

- Logging options
- Session timeouts
- Deep inspection
- Protocol Agents
- Anti-spam
- QoS

Review the Student Guide for scenarios in which these are used.

3.6 The Anatomy of the Policy Editor

The Policy Editor allows you to define rules that control network traffic. These rules have cells (source, destination, service, etc.), each containing specific types of objects. These objects include:

- Host objects (essentially an IP for a host)
- Network objects
- Range objects
- Group objects
- Services (port numbers). Some of these have protocol agents associated with them, denoted by the small blue triangle in the upper left-hand corner of the service icon.
- Users and User groups (Forcepoint User Identification or the Endpoint Context Agent is needed for this)
- Domain Names (a DNS server must be defined in the NGFW properties in order for this to work)
- Network Applications
- Expressions
- Alias objects (most commonly found in templates)

There are many more. Refer to the Student Guide for the complete list. When using the policy editor, generally speaking, objects are dragged and dropped from the **Resource** panel into cells in rules. You can also click into a cell, and type part of the name or number. A list of matching objects will appear, from which you can select. Be familiar with the cells found in the policy and the objects that can be used in each.

3.7 Rule Actions

For every rule you create, there will be an action that you choose, the following is a list of those actions. Please review the Student Guide for more information on their function.

1. Allow
2. Discard

3. Refuse
4. Jump
5. VPN
6. Blacklist
7. Continue

3.8 Options for Rules

When editing rules, there are often configurable options for a particular cell. Most commonly, you will edit the logging options, which can be accomplished by right-clicking in a cell and editing the options. Logging options are particularly important. The following is a list of some of those options:

1. Log Level. The following options are available and should be committed to memory:
    - None
    - Stored
    - Transient
    - Essential
    - Alert
2. In the Logging Options, you can also log Network Applications, User Information, Executable information
3. Allow Options that are available include:
    - Deep Inspection on/off
    - File Filtering on/off
4. Discard Options that are available:
    - Redirection of users. Please review the Student Guide for complete detail.

Please review the Student Guide for additional detail. It is important to understand the relationship of Access Rules and Inspection Rules. There are two ways to approach this:

1. Use the Firewall Template. On a rule-by-rule basis, allow a connection and turn on deep inspection in the Allow Options.
2. Use the Firewall Inspection Template. Continue rules are used to send matching protocols for deep inspection. In this scenario, it would not be necessary to enable deep inspection on a rule-by-rule basis. All you have to do is allow the connection, and the Continue rules in the Firewall Inspection Template take care of sending it for deep inspection.

3.9 NAT

Network Address Translation is designed to translate private to public addresses, or public to private. You have a few options for doing this:

1. Static Source Address Translation
2. Dynamic Source Address Translation
3. Static Destination Translation

Be familiar for the use cases of each. Lastly, when NATing connections, Proxy ARP is designed to make this process more simple. When translating connections to a public IP in a network the firewall owns, it is not necessary to add that IP to the firewall's interfaces - though you could. Instead, Proxy ARP is enabled by default, which allows the firewall to answer on behalf of an IP that is not physically assigned to its interface.

3.10 Policy Activation

When the policy is installed to the NGFW, the entire configuration is sent to the NGFW. This includes:

- The policy
- Any changes to routing or interfaces
- Any changes to the VPN configuration

Other items are sent as well, but the important point is that the SMC maintains the entire configuration of the NGFW (policies, interfaces, routing, etc.). Therefore, very, very little is done at the command line of the engine, apart from troubleshooting. Please refer to the Student Guide for additional detail.

Remember the following :

1. Policy types for each role. Review which rule types are optional for a give role (e.g. if you are not doing any deep inspection in the Firewall/VPN role, then you do not need to associate an inspection policy with the Firewall Policy)
2. There are policy templates for each role. These are designed to save you time and ensure connectivity from engine to management. Although these cannot be edited directly, they can be copied and altered.
3. When creating policy templates, you must create an **insert point**. This defines the order in which rules are processed. Please refer to the Student Guide for additional detail.
4. Review the logging levels and make sure you review the differences between them.
5. Continue rules have several uses. For the purposes of the exam, make sure to understand the scenarios where Continue rules would be useful. They do not make a decision about the connection.
6. Rule order is critical. Rules are processed from the top down. Generally, more specific rules are toward to the top of the policy, and least specific rules are lower in the policy.
7. Review the functions and benefits of using Proxy ARP.
8. Actions and Logging have configurable options. Be familiar with those options, which can be found in the Student Guide.

Chapter 4

Distributed Architectures and NGFW

4.1 Summary

The Forcepoint NGFW Architecture is designed to manage NGFWs, regardless of their physical location. In many cases, there is a central point from which all NGFWs are managed by the SMC. Many of those firewalls will be in remote locations, distant from the SMC. Connections from those remote NGFWs have to be allowed to reach the management server and log server. To do that, NAT is required, as are two other concepts that this chapter covers, Locations and Contact Addresses. These ensure that the NGFWs (and the management client) are using the correct IP addresses (public or private) to communication with system components.

4.2 Key Concepts

- System communication in a NATed environment
- Locations and Contact Addresses
- SMC and NGFW communication ports
- Exchanging data between systems

4.3 System Communication in a NATed Environment

As administrator, if you are at the main office, where the SMC is located, you will communicate with it using its “real“ or private IP address. If you are at home, you would need to use a VPN or communicate with the public IP address of the SMC. The HQ firewall NATs connections from the internet to the SMC using a Static Destination NAT (covered in the last chapter). So, the question is, what IP addresses are used depending on where you are - or where other NGFWs are - relative to the SMC.

The Management and Log servers (the SMC) must be able to communicate with the NGFWs. To do that, you must write rules in the HQ policy that allows those connections from the remote firewalls and NATs them properly.

4.4 Locations and Contact Addresses

- A Location defines what IP addresses will be used for System Communication. Locations are assigned in object properties.
- A Contact Address defines what the IP is - depending on location - that will be used to communicate with a system component. Contact addresses are assigned in object properties. For visual reference, please refer to the Student Guide. There you can see detailed information on where these are configured.

Example uses case:

1. A location is created for “Remote“.
2. An SMC has the IP address of 192.168.10.10 behind the HQ firewall. Therefore, a *public* IP address is defined as the Contact IP address in the Management and Log server properties.
3. In the Management and Log Server properties, you define what IP address is used for things in the “Remote“ location.
4. The “Remote“ location is assigned to all remote NGFWs.
5. If you are at the office, on the same network as the SMC, you set your location to the Default, for which no contact IP was specified. Therefore, you are communicating with the SMC using its “real“ IP.
6. If you at home, attempting to administer the system or at another remote office, you set your location in the Management Client to “Remote“. You will then be communicating using the public IP of the SMC components.

For additional information, please refer to the Student Guide.

Remember the following

1. If there is a firewall between the SMC and remote firewalls, access and NAT rules must be created to permit system communications.
2. Built into the SMC are predefined services that can be used for allowing system communication traffic. Here are some of the most important:
   - **TCP 3020**: This is the port used to monitor the engines as well as receive logs. This must be open between all NGFWs and the SMC
   - **TCP 4987**: This allows the Management Server to control the NGFW
3. Review the Student Guide and know the function of Locations and Contact IP addresses.
4. There is a REST API for communicating with the SMC.
5. Objects can be exported and imported in the form of XML, CSV, and user information can be imported from LDAP.

Chapter 5

NGFW Clustering

5.1 Summary

This chapter covers clustering with the NGFW. The clustering mechanism is designed to be “plug-and-play“, given that no special switch support is necessary. It is important to know all of the terms that are used when referring to clustering. As you learned in the chapter relating to Single Firewalls, there are interface options as well with a cluster. It is necessary to know which ones are only available in clustering.

5.2 Key Concepts

- Firewall Clustering Architecture
- Firewall Clustering Configuration

5.3 Firewall Clustering Architecture

The following are the primary characteristics of the Forcepoint NGFW clustering:

1. The default clustering mode is Active/Active. Although Active/Standby is supported, this would have to be enabled in the General properties of the NGFW.

2. There is a performance increase when a node is added to a cluster. This increase in performance does not really increase beyond five nodes.

3. The clustering does not rely on any special protocols, such as multicast.

4. You can cluster up to 16 nodes together in an Active/Active cluster.

5. Different hardware models can be used in the same cluster (though this is not recommending for continual use).

6. Different software versions can be used in the same cluster (though this is not recommended for continual use).

7. Other clustering mechanisms are supported and includes multicast, multicast with IGMP, and unicast.

8. When upgrading a cluster, this is done “over the wire“ just as with the Single firewall. The SMC takes care of taking a node in the cluster off-line, upgrading it, and bringing back into the cluster so that the same procedure can be performed on the other node. This is done automatically.

9. A Single Firewall can be upgraded to a cluster at any time.

5.4 Terms

It is very important to know all of the terms associated with NGFW clustering. Further, it is important to know what purpose each of these serves.

1. **Packet Dispatch**: this is the name of the clustering algorithm used by the NGFW. This is custom algorithm designed by Forcepoint.
2. **NDI**: this is the Node Dedicated interface. This is type of interface used with the SMC is communicating with the individual cluster members, or nodes.
3. **CVI**: this is the Cluster Virtual interface. This is the addresses to which hosts on the network use when communicating with the firewall. This address is assigned to only one node in the cluster at any given time. The node with the cluster address is referred to as the Packet Dispatcher. Also associated with the CVI is a bogus MAC address. This bogus MAC address should be unique for every set of clustered interfaces and must be unicast.
4. **Packet Dispatcher**: See above.
5. **Gratuitous ARP**: This is an ARP reply for which there was no request. When a node goes off-line, fails, or the load characteristics change in the cluster, the packet dispatcher for that interfaces will change. To quickly update the switch as to the new physical location of the cluster MAC address, a gratuitous ARP is used.
6. **Heartbeat**: This is a set of interfaces that is NOT clustered. The IP addresses assigned to those interfaces must be unique and used nowhere else in the network. These IP addresses can be completely arbitrary as long as they are unique and on the same network.

5.5 Firewall Clustering Configuration

Please review the Student Guide for visual reference on configuring the firewall cluster. Generally, there are few things to keep in mind:

1. For every set of clustered interfaces, a two node cluster will require three IP addresses: one for node 1, one for node 2, and one for the cluster IP address.
2. The heartbeat interfaces are never clustered and should have IP addresses from within the same totally unique network.
3. There are additional interface options that allow you to choose the heartbeat interface and the backup heartbeat interface.

Remember the following

1. The SMC only communicates with NDI addresses.
2. The MAC address assigned to clustered interfaces should be unicast and unique for every clustered interface. A unicast MAC address starts with 00 or an even number.
3. The primary heartbeat network should never be run through the internal network.
4. Expanding a single firewall to a cluster does not impact the SMC license.
5. An NGFW cluster shares the load of processing network traffic, encryption and decryption, deep inspection, and other tasks.
6. Review the packet flow in a cluster found in the Student Guide.

Chapter 6

MSSP and Virtual Engines

6.1 Summary

Managed Security Service Providers are organizations that manage security for other companies. Sometimes this is done through the cloud, and in other cases, on-premise devices are managed remotely by the MSSP. In cases where the MSSP is hosting the physical hardware of the firewall, this chapter will be beneficial. Also, any organization that would like to completely separate the management of different parts of the network will find this equally beneficial. The chapter introduces the concept of Domains and the ability of the NGFW to host independent instances of the NGFW on the same appliance.

6.2 Key Concepts

- SMC Domains
- The Web Portal Server
- Virtual Contexts
- Master Engines and Virtual Engines
- Clustering and Performance
- Deployment and Configuration Example

6.3 SMC Domains

As you have already learned, the SMC is designed to manage all firewalls, virtual and physical. Usually, the firewalls you will manage are yours. However, in the case of MSSPs, they are managing their own security, as well as those of their customers. If you are an MSSP with 400 customers, there are two things you can do. You could create 400 virtual machines and install the SMC on every one - one for each customer. Or, you could install one SMC using the Domain license.

The Domain feature of the SMC allows you to run several completely separate instances of the SMC on the same server. Each of these instances is controlled by the main SMC process, or the Shared Domain. You can think if it as several small Management Servers inside of one big management server. The ability to do this reduces complexity and makes the administration of many customers a great deal more convenient. Using the Domain license saves you from having to create separate SMCs for each customer being managed. Please refer to the Student Guide to see screenshots of how the Domain interface of the SMC appears.

6.4 Web Portal Server

Although this was covered in a previous chapter, here it is of more significance. When managing the security for multiple customers in the same environment, it is impractical, insecure, and unscalable to allow each customer access to the management interface so that they can print reports, see their policies, and review logs. To solve this problem, the Web Portal Server offers a way to allow access to Policies, Logs, and Reports without having to create that customer as an administrator in the SMC. The Web Portal Server has the following characteristics:

1. The installation of the Web Portal Server is done during the installation of the SMC. If it was not installed originally, it can be installed later using the installation software for the SMC.
2. In order to use the Domain features of the SMC, a separate license is required.
3. Logs, Policies, Reports and Policy Snapshots are visible as HTML, read-only.
4. The Web Portal Server's interface can be customized to suit your requirements.

The Student Guide contains a visual reference for how to configure the Web Portal Server through the Management interface. Please review this.

6.5 Virtual Contexts

The NGFW can take on many forms; it can run on a Forcepoint appliance, it can run as a virtual machine or in a cloud-based hosting provider such as Amazon or Microsoft Azure. Any time virtualisation is involved, in the strictest sense, a hypervisor is present.

In the case of Virtual Contexts, however, there is no hypervisor. The NGFW is simply running instances of the NGFW process on the same appliance. Virtual Contexts are assigned physical interfaces from the NGFW appliance. Each instance of the NGFW is completely separate from the other instances. This allows MSSPs or other organizations the ability to get the most out of the hardware. Virtual Contexts can save the cost of having a separate appliance for each firewall being managed. The following is a quick summary of Virtual Contexts:

- Each Virtual Context has its own policy and routing table. For all intents and purposes, it is its own firewall.
- Interfaces from the NGFW appliance are assigned to Virtual Contexts. The Virtual Context uses these interfaces as though they were its own physical interfaces.
- Virtual Contexts are available with the NGFW base license.

Virtual Contexts form the basis for the next section.

6.6 Master Engines and Virtual Engines

As mentioned in the last section, a Virtual Context represents a logical instances of the NGFW. These Virtual Contexts are controlled by a **Master Engine**. A Master Engine is no different from any other NGFW, except that its only mission is to control the resources for Virtual Contexts. The following is a summary of Master Engines:

- The Master Engine is a physical appliance.
- The Master Engine brokers communication from the SMC to the Virtual Contexts, such as logging and engine commands such as policy installation.
- Master Engines can be clustered. The Master Engine Cluster balances the load of processing traffic for all Virtual Contexts. In the case of Master Engine Clustering, the Virtual Contexts are not “assigned“ to a specific node in the cluster. The cluster shares the load of all Virtual Contexts.
- Virtual Engines can perform Access Control, NAT, Deep inspection, etc. Essentially, they have the same capabilities as a physical appliance.

It is important to review the terminology at this point, otherwise things might get a little confusing.

1. A Virtual Context (also known as a Virtual Resource) is created to represent a **Virtual Engine**. The Virtual Context (or Resource) is the object to which physical interfaces from the Master Engine are assigned.

2. A **Virtual Engine** is an NGFW object who's resources, e.g. interfaces and processing, are being controlled by the Virtual Context. A very important concept is that the Virtual Context is the "thing" that is only controlling resources and does *not* appear in the list of managed objects in the Home View. The Virtual Engine - based on the Virtual Context or resource - does appear in the list of managed objects. Managing and monitoring it is no different that managing any other NGFW. There is a specific icon that represents Virtual Engines, clearly indicating that it is a Virtual Engine. **NOTE**: Keep in mind that a Virtual Engine is different from a Virtual Appliance. A Virtual Appliance runs on VMWare or some other virtualisation platform and does appear any differently in the list of Managed engines than a physical appliance.

6.7 Clustering and Performance

As mentioned earlier, Master Engines can be clustered. One important thing to note is that the Virtual Engines themselves cannot be clustered. However, since the Master Engine is clustered and the resources of all Virtual Engines are, in effect, being clustered. The following are some characteristics of Master Engine clustering:

- Each Master Engine can only host Virtual Engines of the same role. For example, you can define to host Virtual Firewall/VPNs, Virtual Layer 2 Firewalls, or Virtual IPS. The roles cannot be mixed on the same Master Engine.

- There are limitations for Virtaul Engines:

    1. Dynamic IP addresses cannot be assigned to Virtual Engines.
    2. Wireless interfaces are not supported with Virtual Engines.

In a recent version, it is now possible to define Layer 2 interfaces to Virtual Engines. In effect, this allows a path to a "mixed mode" Master Engine deployment in that a Virtual Firewall/VPN engine can have Layer 2 interfaces. A maximum of 250 Virtual Engines can be supported by a Master Engine. Clustering a Master Engine has the following benefits:

1. Virtual Engines offer higher performance than NGFWs running on a virtualisation platform such as VMWare.

2. Cluster allows for scalability and assurance. If a node in the Master Engine cluster is taken offline or fails, all Virtual Engines will still be available, as the remaining node in the Master Engine cluster would still be processing for all Virtual Engines.

3. To limit the resources that can be consumed by a Virtual Engine, the maximum interface throughput and concurrent connections can be limited.

For a detailed description of how to configure a Master Engine, please refer to the Student Guide.

Remember the following

1. Virtual Appliances are controlled via a hypervisor, such as in the case of VMWare.

2. Virtual Contexts form the basis of Virtual Engines, in that they are assigned physical interfaces from the Master Engine. When the Virtual Context configuration is completed (in the Master Engine properties), it is used to define the Virtual Engine. The Virtual Engine appears in the list of managed objects in the Home View of the Management Client, just as any other NGFW.

3. Master Engines can be clustered. Each Master Engine has its own Firewall Policy. Usually, the policy that is applied to the Master Engine itself is used to allowed SMC communication.

4. Each Virtual Engine has its own policy, just like any other NGFW. Virtual Engines are almost indistinguishable from other NGFWs, except for the icon that appears in the Management Client.

5. In cases where the number of physical interfaces on the Master Engine is limited, VLAN interfaces can be created on the Master Engine. These can be assigned to a Virtual Context and used by the Virtual Engine as though it were any other interface.

6. Every appliance comes licensed to run Virtual Engines.

7. There is no special license needed to take advantage of Master Engines and Master Engine clusters.

8. The SMC supports the Domain architecture. This is no different from running a normal SMC, except that with Domains, you are essentially running several SMCs inside of one big SMC. These instances of the SMC are referred to as **Domains**. Virtual Engines can be assigned to different domains. As an example, if you are an MSSP with 40 customers, you can use Domains to assign Virtual Engines to different Domains. Each customer, represented by a Domain, is assigned a Virtual Engine from the Shared Domain. This allows you to use one physical appliance to run the NGFWs of many customers. This is a large cost savings.

9. To use Domains, a special license is needed for the SMC.

10. The data contained in each Domain is completely separate from other Domains. For all intents and purposes, each Domain might as well be its own SMC.

Chapter 7

Virtual Private Networks

7.1 Summary

This chapter covers Virtual Private Networks with the NGFW. The focus in this chapter is site-to-site VPNs, in which, generally speaking, private networks are communicating via an IPSec secured channel. Many of the concepts covered can be generalized to any firewall, but there are some aspects that are unique to the Forcepoint NGFW, such as Multi-Link VPN. In this chapter, you should have a general familiarity with IPSec and learn the concepts and terminology unique to the NGFW.

7.2 Key Concepts

- Overview to VPNs
- VPN Topologies
- VPNs and High Availability
- Policy-Based VPNs
- Route-Based VPNs
- VPN Tools
- Hub VPN

7.3 Overview to VPNs

You should review the basic parts of an IPSec VPN connection. In an IPSec negotiation, the firewalls authenticate themselves to each other, then connections are encrypted (usually with ESP), and as this is happening, integrity checking ensures that the packets have not be manipulated in transit. Here are some of the terms associated with that process:

1. IKE (Phase 1)
2. IPSec (Phase 2)
3. ESP

7.4 NGFW VPN Terminology

There are several terms that are specific to the NGFW that will be covered on the exam:

1. **Tunnel**: this represents the VPN connection formed between two or more firewalls over which encrypted traffic flows.
2. **Endpoint**: this is the IP (or IP addresses in the case of Multi-Link) address to which the VPN tunnel terminates on a firewall.
3. **Site**: This is the collection of things that will communicate over the VPN tunnel. This is sometimes referred to as the encryption domain.
4. **Internal VPN Gateway**: this refers specifically to a Forcepoint NGFW that you are managing with your SMC. This is created automatically when you define the firewall.
5. **External VPN Gateway**: this refers to any non-Forcepoint firewall *or* a Forcepoint NGFW that is being managed with some other SMC.
6. **Central Gateway**: this term, and the one that follows, are used in reference to VPN topologies. A Central Gateway is any gateway that is creating and terminating VPN tunnels. This is used mainly in the case of a Full Mesh VPN. In the VPN editor, there are two panes - Central and Satellite. If you drag a VPN Gateway into the Central Gateway pane, then it is a Central VPN Gateway.
7. **Satellite Gateway**: this term appears in reference to VPN topologies. This is most commonly used in Star and Hub VPN topologies, and it represents a single bi-directional path between to VPN gateways.
8. **VPN Profile**: this contains the settings used in the VPN such as IKE settings, IPSec settings, etc. The default VPN profile is “VPN-A Suite“. These can be used for many different VPNs.
9. **Gateway Profile**: this defines the capabilities of a gateway. If the gateway is an NGFW that you are managing, the Gateway profile is selected automatically based on the engine version. If it is a third-party firewall, you may have to define this manually.

7.5 VPN Topologies

The supported VPN topologies are:

1. **Star Topology**: This is also known as a hub and spoke. In this topology, the networks behind the satellite gateways cannot communicate unless you are using the Hub topology. This represents the most common VPN topology.
2. **Full Mesh**: In this topology, all VPN gateways are Central gateway, in contrast to the Star Topology where only one is a Central Gateway, and the others are all Satellite.
3. **Hub Topology**: This is a variation on the Star Topology except that you can use the policy on the Central gateway to forward packets down another tunnel. In this way, you can allow controlled communication between satellite networks.

7.6 VPNs and High Availability

When Multi-Link is used in combination with the VPN, some interesting things become possible. The following is a list of capabilities with a Multi-Link VPN:

- This is only supported with Forcepoint NGFWs.
- When NGFWs are clustered, the VPN Endpoint IP address is the CVI IP.
- VPNs are created in the same way as with a VPN where no Multi-Link was involved.
- In the NGFW properties, the endpoints used in the Multi-Link VPN can be selected or de-selected.

- Endpoint-to-endpoint tunnels are created automatically by the SMC. These are known as “sub-tunnels“. There are 4 modes available for a sub-tunnel:
    1. Active (default)
    2. Standby
    3. Aggregate
    4. QoS-Based link selection
- The mode of each sub-tunnel can be changed.
- Different VPN profiles can be assigned to different sub-tunnels

7.7 Policy-Based VPNs

Policy-based VPNs have the following characteristics:

- Packets are selected based on a match in the Access Rules where the Action is VPN
- Traffic in Policy-Based VPNs is not NATed, by default. Connections bypass the NAT rules.
- In a Policy-Based VPN, IPSec is operating in Tunnel Mode.
- When IPSec is operating in Tunnel Mode, multicast packets are discarded. To use multicast over a VPN, you must configure a Route-based VPN.

Please review the Student Guide for any additional detail.

7.8 Route-Based VPNs

Route-based VPNs have the following characteristics:

- Packets are selected based on the routing table
- You must add a tunnel interface to the NGFW so that packets from the Route-based VPN are encapsulated. You can choose GRE, IP-in-IP, SIT, or VPN for encapsulating the packets.
- Packets in a Route-based VPN are processed against the NAT rules. Therefore, in order to allow network-to-network connections across the VPN using their real IP addresses, must create Empty NAT rules to prevent the traffic from being NATed.
- Route-based VPNs operate in Transport Mode. Because of this, Route-based VPNs allow multicast traffic. If you wish to use any multicast traffic (e.g. OSPF, BGP) over the VPN, you must use a Route-based VPN.
- In the Access rules, the Action to allow this site-to-site communication is Allow - since the routing table selects packets for encryption.
- The routing table of the engine must be adjusted to add the remote network to the tunnel interface.

Please review the Student Guide for any additional detail.

7.9 VPN Tools

There are a number of tools available to help you use and get information about your configured VPNs. Please refer to the Student Guide a additional information.

7.10 Mobile VPN

In the course material and in the Student Guide, Mobile VPNs are covered in a separate section. However, since we are on the topic of VPNs, we have included the information here. Mobile VPNs fall roughly into two categories:

1. **IPSec Mobile VPN**: in this case, there is a dedicated Windows VPN client that supports both IPSec and SSL VPN. Other VPN clients will work for IPSec, e.g. the Mac VPN client can be configured to operate with the NGFW. A client is required for this. When the client is used for IPSec or SSL, the user can have full network access. IP addresses can be assigned from the internal network to the virtual adapter of the VPN client.

2. **SSL VPN**: the SSL VPN secures communication through SSL. This is a lighter weight alternative to IPSec. The main difference between the IPSec and SSL VPNs is the fact that the SSL VPN can be clientless. Built into the NGFW is an SSL VPN portal. Users would access the portal with a web browser, allowing them to access **web-based** services only. The same Windows VPN client can be used for both SSL VPN and IPSec. When full network access is required for the SSL VPN, the client must be used. The SSL VPN client is supported for Mac, Windows, and Android.

Both the IPSec and SSL VPN clients support a variety of authentication mechanisms, both internal and external. Remember that Internal authentication mechanisms are those that are supported by the SMC, and external authentication mechanisms are those supported by other things such as RADIUS. An example of an external authentication mechanism would be the Network Policy Server (NPS) or RSA tokens.

Please refer to the Student Guide for a complete list of supported authentication mechanisms for IPSec and SSL VPN connections.

7.10.1 VPN Client Address Management

In order for a VPN client to have full network access, with either SSL or IPSec, an IP address is needed. There are two ways to manage VPN client addresses:

1. **Virtual Adapter**: using an external DHCP server, located on the private network, an address can be assigned to a virtual adapter that is installed when the VPN client software is installed. When a user successfully authenticates, an address is sent from the DHCP server on the internal network to the Virtual Adapter at the client end of the connection. After that, the user can access internal resources as defined in the policy. The advantage to using the virtual adapter is that users can distinguished from each other, as they have their own unique IP address.

2. **NAT Pool**: this method of client address management has the advantage of being easy to use and fast to set up. When a client connects to the VPN, they are NATed to an IP address on the internal network. You can think of this as like a dynamic source NAT in reverse. If there are many VPN clients, then they call appear to come from the same address. The disadvantage to this is that it is not possible to distinguish the users based on IP addresses.

Remember the following

1. Know the VPN topologies.

2. Policy-based VPNs are used with unicast traffic; Route-based VPNs are used for either unicast or multicast.

3. Review the terminology listed above.

4. The VPN Profile decides the settings for a given VPN. It defines the settings for IKE (Phase 1) and IPSec (Phase 2).

5. In VPNs between a Forcepoint NGFW and a third-party firewall, a pre-shared key must be selected for authentication.

6. Know the different ways in which packets are selected based on the VPN types.

7. In the access rules, the VPN action has options. These are Enforce VPN and Apply VPN. Review the Student Guide for additional detail.

8. Both IPSec and SSL VPNs are included in the base license of the NGFW.

9. When Multi-Link is used, the mobile VPN client can re-establish the VPN tunnel on the other ISP should the primary fail.

10. Full network access with a Mobile VPN can only be achieved through the use of the VPN client. In the case of the SSL VPN portal (clientless), only access to web-based resources is supported.

Chapter 8

Traffic Management

8.1 Summary

The Forcepoint NGFW allows you to control network traffic in a number of ways. In the context of Multi-Link, we are referring to connecting multiple ISP connections to the NGFW. When this is done, you have more control over where traffic is going, both inbound and outbound. Multi-Link is how this is done. Traffic can be load-balanced between ISPs, and you can ensure that your domain is always resolving to the most accurate set of IP addresses.

8.2 Key Concepts

- Outbound Traffic Management
- Link Selection Methods
- Outbound Multi-Link configuration

8.3 Outbound Traffic Management

With the Forcepoint NGFW, outbound traffic management refers to Multi-Link. Multi-Link provides the following:

- Dynamic load balancing across multiple ISP connections. There is no limitation to this.
- ISPs can be aggregated for better bandwidth.
- Used with the VPNs, Mutli-Link provides a very robust and fault tolerant connection.
- Only IPv4 is supported.
- Failover is NOT transparent, as the source addresses must change when the connections fails over to another ISP.

8.4 Link Selection Methods

Packets can be selected for an ISP based on three different methods:

1. RTT: this is round-trip time of a SYN packet. Primarily used with the bandwidth of all ISPs is similar. Please refer to the Student Guide for additional detail.
2. Ratio: with this method, the firewall must know about the speed of each ISP. It then computes a ratio of the speeds, and distributes the traffic accordingly.

3. QoS: this offers a great deal of control over the ISP used by a particular type of traffic. Matching Access rules with QoS defined will assign traffic to an ISP designated in the Multi-Link configuration. Please refer to the Student guide for additional detail.

8.5 Outbound Multi-Link Configuration

For a visual understanding of configuring Multi-Link, please refer to the Student Guide. For the exam, please review the terminology below:

- **Netlink**: this is an object that defines a path to the internet (in the case of ISP load balancing). It is based on the router object that represents the next-hop router for that ISP.
- **Outbound Multi-Link Object**: This is used to combine Netlinks together for outbound load balancing (ISP load balancing). Outbound Multi-Link objects are used in Dynamic Source NAT rules.

The order of operations for defining Multi-Link is the following:

1. Add an interface to the firewall that represents the new ISP.
2. Create the router object(s) that represent the next hop router for your ISP.
3. Use those router objects to create the Netlinks, one for each ISP.
4. Add the Netlinks to the appropriate interface in the Routing view of the NGFW properties and set them as the default route.
5. Create the Outbound Multi-Link object, using the Netlinks. It is here that you specify the IP address to which outbound connections on that ISP are NATed.
6. Create a Dynamic Source NAT and select the Outbound Multi-Link object as the thing to which connections are NATed. This activates the outbound ISP load balancing.

Remember the following

1. Know the limitations of Multi-Link mentioned above.
2. Review the Student Guide and read the details for the outbound load balancing methods. Also, be sure to know all of them.
3. The order of operations for configuring Multi-Link is important. Review the object types listed above and their role in the Multi-Link configuration.

PART II

SECURITY

Chapter 9

Authentication and User Identification

9.1 Summary

Having user information available in the SMC is very beneficial and it allows you to take advantage of several NGFW features. With user information, you can control network access based on user information, have deep visibility into the actions of users on your network, and enforce authentication for access to network resources. There are two different ways to get this information, the Forcepoint User Identification or the Endpoint Context agent.

9.2 Key Concepts

- User Management and Authentication
- Directory Server Integration
- Forcepoint User Identification
- Endpoint Context Agent
- User Monitoring

9.3 User Management and Authentication

The SMC can get user information from two places: external directory servers, such as Active Directory, or from an LDAP database that is built into the SMC. User information is stored in a directory server. This is usually Active Directory or OpenLDAP. In order to get this information, the following must be done:

1. Create an object to represent the directory server. There are built-in objects for Active Directory and OpenLDAP. Please refer to the Student Guide for a more visual representation of this process
2. Create a domain in the SMC to represent the domain for which the Directory server is providing information, and set it as the default domain for users.
3. Use the users and user groups in Access rules for User-based access control or for authentication.

The Internal LDAP database that is built into the SMC is primarily used in smaller locations when Active Directory might be impractical.

When the user information is available, you can do one or both of the following things:

- Authenticate Users
- Control users access to network resources by using them as the source or destination in Access rules.

9.3.1 Authentication

Users are authenticated according to methods supported by the directory servers and the NGFW. Here are the supported authentication methods based on which directory server is to be used:

- Internal Authentication: these are authentication methods supported by the Internal LDAP database on the SMC. These include:
  1. User Password
  2. Certificate
  3. Pre-shared key
- External Authentication methods include:
  1. RADIUS
  2. TACACS+
  3. Network Policy Server (part of AD, similar to RADIUS)
  4. LDAP Password

Please refer to the Student Guide for additional information on the communication process between the NGFW and the directory servers.

When the user information is available (after the integration with the directory server), the Authentication cell of the Access Rules may be used to select which users must authenticate and how.

9.3.2 User-based Access Control

User-based access control uses the Forcepoint User Identification Service to resolve a user to an IP address. In this scenario, the firewall communicates with FUID directly so that it is always aware of a user's current IP address. The user or user group is used in the source and destination columns of access rules. In essence, the user is being converted to an IP address. The following is a list of the FUID components. Please refer to the Student Guide for detailed information. For the purposes of the exam, a basic understanding is required.

1. Directory Aggregation Service
2. DC Agent
3. UID Service

The DC Agent is installed on Windows and monitors user IP address information, which is sent to the User ID Service. The Directory Aggregation Server and the User ID Service is installed on a Linux machine, typically CentOS. The Directory Aggregation Server monitors the domain User and User Group information, which is also sent to the User Identification Service.

9.4 Endpoint Context Agent

In addition to using FUID, there is another way to get user information. The Endpoint Context Agent, which is installed on an endpoint, provides user information directly to the NGFW. Because the agent lives on the endpoint, information about the user, the operating system, installed applications, and system information are available to the NGFW. The following are the characteristics of the Endpoint Context Agent:

1. The Endpoint Context Agent must be installed by the endpoint local administrator.
2. It support only the Windows operating system, currently.
3. It collects metadata about information on the endpoint. For a complete list of information sent to the NGFW, please refer to the Student Guide.

The information collected from the endpoint is then used to make various access control decisions. Its strongest use case is controlling which installed applications on the endpoint are allowed to generate network traffic. Built into the SMC is a large list of endpoint applications. Those can be used in the source and destination columns of access rules.

Remember the following

1. Review the configuration process for integrating Active Directory with the SMC. For example, know that the Bind User ID and Bind user password are required for the SMC to read the user directory.

2. The Internal LDAP database built into the SMC automatically replicates to the NGFW so that the NGFW has a local copy of the LDAP database. This makes authentication quite fast, as the NGFW does not have to communicate with an external directory server. The Internal LDAP database has the limitation of not being scalable to the large enterprise, which would likely already have Active Directory.

3. The use of Forcepoint User Identification and the Endpoint Context agent is part of the base license of the NGFW, i.e. you do not need an additional license for these features.

4. The Endpoint Context Agent requires a unique certificate for each endpoint. There are two ways to distribute those certificates, manually or through the use of Active Directory's Certificate Auto-Enrollment service.

Chapter 10

Extended Connection Controls

10.1 Summary

In addition to having additional information to make traffic control decisions, it is also useful to have other information about a connection. Some of this vital information can be found in the payload of a packet. This information can be used by the NGFW in a number of ways, not the least of which is Deep Packet Inspection. Deep Inspection is the process of decoding a packet up to the application layer. Information contained there can also be used for Network Application Identification, Protocol Agents, and File Inspection. This chapter covers an introduction to Deep Inspection.

10.2 Key Concepts

- Review of connection controls
- Services and Services with Protocol Agents
- Sidewinder Proxy Modules
- Network Applications
- Network Applications vs. Endpoint Applications

10.3 Review of Access Control Methods

There are a number of access control methods that have already been covered. If you would like additional details for any of these, please refer to the Student Guide.

- Anti-spoofing
- Geo-protection (based on a list of currently assigned IP blocks by country)
- Basic access control based on things that can be resolved to IP addresses (hosts, networks, ranges, expressions, aliases, etc.)
- Stateful Connection Tracking
- User Access Control

The other ways of controlling connections are:

- Proxy Modules
- Deep Packet Inspection

10.4 Services and Services with Protocol Agents

- **Services**: these represent port numbers. For example, the HTTP service object is defined for port 80.
- **Service with a Protocol Agent**: A small blue triangle in the upper left-hand corner of the service icon denotes that there is a Protocol Agent in use for that service. A Protocol agent helps the connection in some way. Some examples are:

  1. Ensuring the proper NATing of connections
  2. Validating a protocol
  3. Opening ports dynamically as necessary for certain protocols.

  For a complete list, please refer to the Student Guide. In all of these cases, decoding further up the stack, past Layer 4, is required.

10.5 Sidewinder Proxy Modules

When a service matches in an access rule, the connection is simply allowed. The NGFW tracks the state of the connection, performs deep inspection (if configured), and other validations. However, the connection is still flowing between the two endpoints of the connection without interruption from the firewall. In certain cases, it is useful to control very, very specific aspects of a protocol, such as the allowable methods in HTTP. To do this, a proxy is needed. The NGFW currently supports the following proxy modules:

- Generic TCP
- Generic UDP
- HTTP
- HTTPS
- SSH
- FTP

Please refer to the Student Guide for a visual representation of how these are configured. When a connection matches a rule where a proxy service is used in the Service cell, the firewall interrupts the connection and initiates a new one on behalf of the requesting host. In this way, the NGFW has complete control of the connection.

10.6 Network Applications

Network applications are simply signatures that identify the use of a network (typically http or https) application such as Facebook, Twitter, Salesforce, etc. Here are the characteristics of Network Applications:

- Network applications are defined with a port number. Editing the service cell and combining a network application with the “TCP Any Service“ element overrides the default port number so that the NGFW ignores the port number and looks for an application regardless of port.
- Network Applications that are found in HTTPS connections can still be identified using a TLS match. Simply put, certificate information about a HUGE list of domains is built into the SMC. The NGFW can compare this to the certificate presented during SSL negotiations and identify the application based on that certificate match. This prevents the need to decrypt. If there are network applications that run inside of an already encrypted connection (such as Facebook Chat), decryption would be required.
- Network applications can be used in the service cell of an Access Rule for controlling traffic, or Network Application logging can be turned on in the Logging options just for reporting purposes.

- Network applications differ from Endpoint applications in that Network applications are identified based on the network traffic flowing through the firewall. Endpoint applications are identified and reported to the NGFW from the endpoint context agent. An Endpoint Application signature looks at characteristics of applications that would be installed on an endpoint such as InternetExplorer.exe or Firefox.exe. The SMC maintains a list of these network and endpoint application signatures that are updated via the SMC dynamic update packages.

For additional information on the above items, please refer to the Student Guide.

Remember the following

1. Services without protocol agents are just port numbers.
2. Protocol Agents are associated with many services by default. The Protocol Agent is activated automatically when the service matches.
3. Proxy Services actually break the original connection and create a new connection on behalf of the original requesting host. This gives the firewall maximum control of the connection.
4. Network applications can be used for just logging and they can be used to make access control decisions.
5. TLS matches help to identify encrypted applications.
6. Network application logging is enabled in the Logging options of a rule.
7. There is no additional license needed to use Network and Endpoint application.
8. Review the Student Guide for additional detail on configuring the use of Sidewinder Proxies and Network Applications.

Chapter 11

Deep Packet Inspection

11.1 Summary

To extend from the previous chapter, this chapter will cover the process of how the NGFW identifies malicious traffic. As you have already seen, deep inspection is vital to any Next Generation Firewall. However, there is far more to it. This chapter will how the deep inspection process works, the strategies you can use for deep inspection, and the Inspection Policy anatomy.

11.2 Key Concepts

- Deep Inspection with the NGFW
- The Inspection Policy
- Predefined Inspection Policies
- The Inspection Rules tree view
- Fine-tuning deep inspection
- Exception Rules in Inspection Policies
- Blacklisting

11.3 Deep Inspection with the NGFW

The basic characteristics of deep inspection with the NGFW are listed below:

- Protocol Validation ensures that the protocol is working as intended, and helps with other aspects of the connection as listed in the previous chapter.
- Matching traffic against patterns of known exploits.
- Custom fingerprints can be created.
- Fingerprints (signatures) are based on Regular Expressions
- Dynamic Updates, which are released by Forcepoint periodically, contain any updates, additions, or removal of fingerprints.
- All roles are capable of deep inspection, and the NGFW base license enables all roles to perform full deep inspection.

Packets are sent for deep inspection based on matches in the Access Rules. If you are using the Firewall Template, no connection is sent for deep inspection by default. To send a connection for deep inspection, in this case, you edit the **Allow** action options and enable deep inspection. When the rule matches, and the connection is allowed, the firewall will process the connection against the Inspection policy that you have selected. See below for more information.

If you are using the Firewall Inspection Template, there are Continue rules in the template that send a large number of services for deep inspection. In this case, all you have to do is allow the connection in the normal way. If the allowed protocol is one that is being sent for deep inspection by the Firewall Inspection Template continue rules, then that connection will be automatically sent for deep inspection.

11.4 The Inspection Policy

The Inspection Policy is a collection of rules that contain signatures of attacks. The Inspection Policy is maintained separately from the Firewall Policy, which make both easier to read, and allows you to switch between Inspection Policies very quickly should the need arise. In the firewall's policy, there is the "Inspection" tab. It is there that the Inspection Policy is selected.

As with the Firewall Policies, there are two templates that you can use for Inspection Policies:

1. Medium Security Inspection Template
2. High Security Inspection Template

Both of these can be used as a starting point when creating your own Inspection Policy. For a detailed explanation of the differences in these templates.

11.5 Situations

Situations are patterns of interest, and in the case of deep inspection, signatures contain patterns of known malicious activity. It is important to remember that Situations can be generated by two things:

1. System Situations that are raised as the result of something to do with the SMC, engine, etc.
2. Situations can be raised as a result of a pattern match to a known attack.

In any case, Situations are associated with the following:

- Context
- Tags
- Vulnerabilities
- Types

Please refer to the Student Guide for a detailed explanation of each of these. Of these, the Context is the most important as it pertains to Situations. By defining the Context of the connection, the NGFW knows where the pattern of attack is mostly likely to occur in a connection. For example, if you wanted to write a signature that looked for failed login messages from an FTP server, you would expect to see that failed login message come from the FTP server. Therefore, the context of the connection is FTP server Stream.

11.6 The Inspection Rules Tree View

When editing an Inspection Policy, there are two tabs:

1. Exceptions Tab
2. Inspection Tab

The Exception Rules are processed before the Inspection Rules tree. Any custom situations, rules to clean up false positives, and rules that pertain to specific sources and destinations are used in the Exception Rules. These rule are similar to Access Rules, but they contain additional columns. Please review the Student Guide to see the columns that are present in the Exceptions Rules.

The Inspection Rules tree contains a list of the all signatures present in the system and available to the NGFW. The action taken by the NGFW for each Situation is specified for each type. The Rules Tree does not allow you to limit the scope of a change to a signature. For example, if there were two database servers that were generating a false positive, you would not be able to change the action of that signature just between those two hosts. To do that, the Exceptions Rules would be used.

Please make sure to review the Student Guide and study the anatomy of the Exceptions and Inspection rules. Identify the columns that appear there that are not present in Firewall Access rules.

11.7 Blacklisting

Blacklisting is used to automatically block a source IP address for a specified period of time. The following are characteristics of Blacklisting:

- Blacklisting is done by system components sending information about a connection that should be blacklisted for a period of time to *Executors*.
- Blacklists can be requested by the SMC or other NGFWs in your environment.
- Blacklists are meant to timeout after a period time specified in the Blacklist request.
- Blacklist entries can be deleted through the Management Client, allowing traffic to flow again.
- A policy push is not required for a Blacklist to take effect - it is an automatic process.

Blacklisting can be manual, i.e. created by the administrator through the Management Client, or they can be automatic. In order for automatic blacklisting to work, a rule must be added in the Access or Inspection rules to blacklist a connection when certain criteria are met.

Blacklisting is useful in the following situations:

- When an NGFW is in IDS mode and cannot directly stop the connection. Information about the offending connection is sent to an NGFW that can block the connection.
- To stop attacks that have many parts, such as a brute force password attack. Each failed login is not an attack in and of itself, but 50 failed logins in a space of 10 seconds is an attack. Information about the source of this attack can be used to blacklist all traffic from that source.

Remember the following

1. There are two ways to send traffic for deep inspection:
   (a) Use the Firewall Template and send connections for inspection on a rule-by-rule basis.
   (b) Use the Firewall Inspection Template where Continue rules are used in the template to send a large number of protocols for deep inspection by default. When using the Firewall Inspection Template, connections are simply allowed in the Access Rules. The Continue Rules take care of sending the matching connection for deep inspection.
2. Actions used in Inspection Rules are:
   (a) Permit
   (b) Terminate
   (c) Refuse
   (d) Apply blacklist
3. Situations are based on Regular Expression. Review the Student Guide for additional detail on Regular Expressions.

4. Continue rules do not *automatically* send matching connections for deep inspection. They set a value for the matching connection that sends it for deep inspection *only if it is allowed by an Access Rule further down in the policy. Remember that Continue Rules do not make a decision about a connection. They specify how the connection is handled if it is allowed further down in the policy*

5. Review all of the connection controls mentioned in the Student Guide.

Chapter 12

Malware Detection and File Filtering

12.1 Summary

As you have already seen, there are a number of different policy types that you can use. The main policies are Firewall Policies, Layer 2 Firewall Policies, and IPS Policies. You have seen that for each of these, you can associate other policy types, e.g. Inspection Policies, that extend the functionality of the NGFW. To further extend the capabilities of the NGFW, this chapter will cover File Filtering policies as a way to block files from introducing a threat to the network. In addition to using a File Filtering policy, you will also see how the NGFW can work in conjunction with one of the Forecepoint Cloud Services to further enhance to ability of the NGFW to detect malware.

12.2 Key Concepts

- Malware Detection Process
- The File Filtering Policy
- File Reputation Service
- Embedded Anti-Malware scan
- Advanced Malware Detection

12.3 Malware Detection Process

In the last chapter, you looked at how the NGFW can identify attacks using a number of different methods, largely centered around signature (situation) matches. However, signature matching is one part of defending the network. Another part of defending a network is to block vectors of attacks such as an infected file. The NGFW has to examine many aspects of the file, and when you consider what it takes to examine a file (memory, resources, etc.), the NGFW benefits greatly from being able to utilize other methods of detecting attacks in files. Below are the basic steps of the process:

1. If you enable it, in the Global System Properties, the NGFW receives a file, computes of hash of it, and then queries McAfee GTI (Global Threat Intelligence).
2. The NGFW can then process the file against the embedded anti-malware scan.
3. If there is still no determination of the nature of the file, then the NGFW can forward to the file to Forcepoint Advanced Malware Detection. This is a sandboxing service (or on-premise device) that will unpack the file and observe its behavior when opened.
4. Depending on the outcome of these checks, the file may be discarded or allowed.

In much the same way as deep inspection is enabled for matching connections, the same hold true for file filtering. Here are the approaches to file filtering:

1. Using the Access rules, connections can be sent for File Filtering in the Allow options. This allows you to turn on file filtering on a rule-by-rule basis.
2. Again, using the Access rules, a Continue rule can be used to send matching connections for File Filtering, provided that the connection is allowed further down the rule base.

NOTE: In order for File Filtering to work, it must be enabled in the “Add-Ons“ section of the NGFW properties.

12.4 The File Filtering Policy and Reputation

The File Filtering Policy is very similar to other rules. There are additional columns, however, that are specific to File Filtering:

- **File Type**: this is the type of file that you wish to examine. There are a number of these built into the SMC. Please refer to the Student Guide for additional information.
- **Allow After**: this is not an additional cell, this is an action that is specific to File Filtering. Essentially, this means that a connection containing a file will be allowed after a certain set of criteria are met.

The available checks that you can perform on a file are:

- McAfee GTI file reputation scan. **NOTE**: unlike other Forcepoint Cloud Service integrations, using McAfee GTI does not require a separate license.
- Embedded Anti-Malware scan. This is built into the NGFW and provides another layer of checking prior to allowing a file. There is no additional license necessary to use this feature.
- Advanced Malware Detection (on-premise or Cloud)

In any of these cases, there is a reputation that returned. Depending on that reputation, there are sliders in the options of the **Allow After** action that allow to decide which reputation would allow a file and which one would discard it. The options for reputation are:

1. Malicious
2. Unknown
3. Trustworthy

You appetite for risk can be adjusted by moving the sliders. For detailed information on this and to see a screenshot of the configuration, please refer to the Student Guide.

There are several protocols over which files can arrive into your network. The following is a list of supported protocols for File Filtering:

- HTTP
- HTTPS
- FTP
- SMTP
- POP
- IMAP

12.5 Advanced Malware Detection

One of the goals of using external inspection mechanisms such as Reputation Services is to reduce the amount of work the firewall has to perform when inspecting files. For example, if there were a great many files coming into the network simultaneously, the NGFW would be very bust attempting to inspect them all. For that reason, Reputation Services allow the NGFW to do the following:

1. Compute a has of the file.
2. Send that hash to GTI or Forcepoint (or both) to determine if the file has been seen before and what the associated risk level is like for that file.
3. When GTI returns unknown and when Forcepoint returns unknown, then the only way to determine what the file could contain is to model its behavior with Advanced Malware Detection.

If the answer from the Reputation services is “Unknown“, then Advanced Malware Detection can be used to make a definitive determination about the file.

NOTE: There could be cases in which AMD cannot make a determination about the file. If this is the case, then you can decide what to do. Please refer to the Student Guide to see how the configuration for this works.

Much like other aspects of File Filtering, AMD must be enabled in the Add-On section in the NGFW properties.

Remember the following

1. There is a specific type of policy to perform File Filtering. Just like the Inspection Policy, this is associated with the main policy on the **Inspection** tab.
2. There is an additional action in File Filtering policies called “Allow After“. This ensures that connections are allowed on;y after they have passed the checks that you configure in the Allow After options.
3. McAfee GTI does not need an additional license.
4. File Filtering, without the use of any additional Forcepoint service, does not require an additional license.
5. Using the Forcepoint File Reputation service or Advanced Malware Detection does require an add-on license.
6. Files can be sent for File Filtering on a rule-by-rule basis, or you can use a Continue Rule in the Access Rules to send matching connections for File Filtering. Please review how to use Continue rules and understand their effect on traffic that matches them. (Think of it like this: if there is a rule where the Source is Network A, the destination is Network B, the Service is HTTP, and the Action is Continue. When a connection matches the Continue rule, that traffic is NOT immediately sent for inspection. It will be sent for File Filtering if, and only if, that traffic is allowed by an Access Rule further down in the Access Rules.)
7. To use Advanced Malware Detection, you must have the Add-on license for the NGFW and the appliance key and token for the AMD cloud service or on-premise appliance.

Chapter 13

Inspection Techniques

13.1 Summary

In Chapter 10, you got an introduction to Deep Packet Inspection, and you explored it from the perspective of Inspection Policies and getting connections from Access rules to Inspection rules. Here, you will dig deeper into the concept of how the NGFW does deep inspection. You will explore how the NGFW examines streams of traffic and performs one of its most important tasks, Evasion Prevention. Lastly, you will explore Regular Expressions and their role in the deep inspection process.

13.2 Key Concepts

- NGFW Inspection Techniques
- Traffic Inspection Process
- Advanced Evasion Detection (normalization)
- Misuse Detection with fingerprints
- The Concept of Situations
- Regular Expression Syntax

13.3 NGFW Inspection Techniques

In earlier chapters you got a basic introduction to deep inspection. You established that Inspection policies are associated with Firewall, Layer 2 Firewall, and IPS policies. You also learned that editing the options for the **Allow** action enables you to send connections for processing against the Inspection Policy. There are several techniques that are in use when inspecting traffic. The following is a list of those techniques:

- **Misuse Detection**: patterns of known attacks are matched against the traffic.
- **Malware Detection**: traffic is examined for files entering or leaving the network. File Reputation checking, Anti-Malware (built into the NGFW), and AMD (Advanced Malware Detection) are used to examine the traffic for signs of malicious content.
- **Protocol Validation**: ensures that traffic is not behaving in a way that may not be permitted by the standards of the protocol. In some cases, an attack is so new that there is no signature for it. In these cases, Protocol Validation can identify “Zero-Day“ exploits if they violate some aspect of the protocol.

- **Traffic Anomaly Detection**: when signatures and other methods are not enough to detect malicious activity, the NGFW can detect when traffic deviates from a “normal“ profile through the use of statistical triggers. An example of this is Denial of Service protection built into the NGFW, e.g. SYN flood detection and prevention.
- **Protocol Anomaly Detection**: although related to Protocol Validation, Protocol Anomaly Detection normalizes the connection so that anything that is ambiguous or malicious can be identified or resolved. Another part of Protocol Anomaly Detection is, as you have learned earlier, is Stateful Inspection. By keeping track of the connection and what part of the connection to expect, the NGFW can easily detect any anomalies in the traffic.

Please review the Student Guide for additional detail.

13.4 Traffic Inspection Process

In order to detect attacks accurately, the NGFW examines with increasing specificity. At a high level, here at the steps for the inspection process:

1. Traffic that has been allowed by an Access rule is sent for deep inspection. Remember that this can be done with a Continue rule or done on a rule-by-rule basis.
2. Traffic Normalization is performed. Traffic Normalization is a process wherein the NGFW resolves or removes anything that would make inspection the traffic difficult or impossible. A common example of normalization is a case where the NGFW receives fragments of a packet or connection. Normalizing that connection would be waiting on all parts of the packet or segment before performing analysis. Attempts to evade the NGFW can be detected with normalization.
3. In order to ensure a fast and accurate match to traffic, the NGFW divides traffic by protocol.
4. Within a given protocol, the NGFW uses other pieces of contextual information to ensure accurate signature matches, such as what part of the protocol is to be examined, e.g. HTTP Server Stream or FTP Client stream.
5. Lastly, once the traffic has been divided into protocol, the context of the traffic has been considered, the NGFW can now match the most relevant patterns of attacks to the traffic being examined.

For each of these, briefly review the Student Guide for more context and a graphical representation of how traffic is “sifted“ or filtered prior to the pattern match.

13.5 Advanced Evasion Techniques

This section and the previous section are related by Normalization. In a nutshell, traffic moving over the internet is being sent according to some protocol that is governed by an RFC. Many protocols do not follow the RFC to the letter, perhaps due to differences in operating systems or just a sloppy implementation. In either case, the NGFW has to examine the traffic and decide what aspects of the connection are needed for delivering a packet to the intended destination and what parts of the packet are, in the best case, superfluous, and in the worst case, malicious. Protocols can be manipulated in such a way that firewalls may not recognize the connection or fail to react to the connection carrying a malicious payload.

There are endless possibilities for creating evasions. Packets and connections can be manipulated in so many combinations that having signatures for all possible evasions would be impossible. Normalization ensures that packets are delivered as they should be, and things that are ambiguous or unusual are filtered out.

While the System Engineer exam does not cover this topic in great detail, it is recommended to review the Student Guide for additional examples of evasions.

13.6 Misuse Detection with Fingerprints

The most widely known way of identifying attacks is through the use of fingerprints. They go by many names - fingerprints, signatures, situations - but they all mean the same thing, a pattern of a known attack. There are many different ways to write signatures, some being faster than others. The Forcepoint NGFW uses the **DFA**, or **D**erterministic **F**inite **A**utomaton. These offer a speed advantage over other methods of inspection. Please refer to the Student Guide for more detail.

13.6.1 Situations Concept

As a follow-on to the previous section, Situations, in the context of deep inspection, represent patterns of attacks. Situations have the following elements associated with them:

- **Context**: as stated above, the Context is the *part* of a connection of a given protocol where the NGFW will focus to find a particular attack. For example, if the signature is looking for an attack from a client connecting to an HTTP server, the NGFW would focus on the client stream traffic and ignore other aspects of the connection. This increases the speed and performance of the NGFW and reduces the likelihood of false positives.

- **Tags**: these are assigned to situations that have something in common. For example, there is a tag called “Not Latest Browser Versions“. There are many situations with that tag - all having in common the fact that they are not the latest version of a given browser. Tags can be used as matching criteria in Exception Rules (the first tab in an Inspection Policy).

- **Vulnerabilities**: for a given Vulnerability, you can quickly see all of the Situations that are related. Please refer to the Student Guide for information on the relationship between the Severity and the Vulnerability.

- **Type**: refers to a classification scheme used in the Inspection Rules Tree. Each Situation or signature is associated with type such as “Suspicious Traffic“, “Attacks“, or “Botnet“. By examining the Inspection Rules Tree screenshot in the Student Guide, you can see the full list of Types.

13.7 Regular Expressions

In this chapter, you have reviewed the techniques used by the NGFW for identifying attacks. While things like Protocol Validation and Normalization happen largely in the background, Situations (fingerprints) are more tangible. If you examine a Situation used for identifying attacks, you will likely see what appears to be where someone dropped their keyboard. In reality, these seemingly random mixes of slashes, dots, asterisks, and more are actually something known as **Regular Expressions**.

There is an entire universe of information about Regular Expressions available. It would take some time to cover all there is to know about them. However, once you learn the syntax for Regular Expression, you can use them to *describe* anything you would like to find in a string of traffic. After the NGFW has identified the context of the traffic, it then matches that traffic against a fingerprint - which is the Regular Expression. Please review the Student Guide for a basic introduction to Regular Expression syntax. For the exam, it is not necessary to be an expert. The chart that appears in the Student Guide will help.

Remember the following

1. Situations is a somewhat broad term that also includes things related to system functioning. For example, if the disk on the Log Server was about to be full, a Situation would be raised to let you know. In the context of Deep Inspection, Situations refer to patterns of known attacks.

2. Just because there isn’t a signature for some attack, you are not necessarily defenseless. Protocol Validation, Protocol Anomaly Detection (Normalization), and Traffic Anomaly detection can help identify threats, even when there is no Situation for it.

3. The Context of a given connection allows the NGFW to limit where it is attempting to identify an attack. If you were looking for failed login attempts to an FTP server, then you would expect to see that message from the FTP Server Stream - which is the Context you would use for this custom situation.

4. Advanced Evasion Techniques is any type of attack that would attempt to bypass the firewall. There are countless ways to do this, but Full Stack Normalization (performed by the NGFW) would identify them. These techniques often make creative use of arcane capabilities in a protocol that many firewalls fail to recognize.

5. Regular Expressions are like anything other programming language - there is a syntax that can be learned. The goal of using Regular Expressions is to use its syntax to concisely and completely describe the thing you are looking for. The more specific and concise they are, they faster they perform. Limit the use of “.*“ (that is “dot star“) in you Regular Expressions. That means to match any character an infinite number of times.

6. The Inspection Rules tree breaks down Forcepoint Situations by type.

Chapter 14

Inspecting TLS

14.1 Summary

TLS, or Transport Layer Security, is used when traffic needs to be secured by encryption. While being useful for protecting legitimate communication, it can also hide attacks. By default, most firewalls do not decrypt traffic due to privacy concerns or performance impact on the firewall. As with deep inspection, decrypting SSL can be performed on a rule-by-rule basis, allowing you to use it surgically. TLS inspection is designed to address the possibility that malicious traffic could arrive over an encrypted channel. TLS inspection is also very useful for identifying network applications that are encrypted. As you might remember from a previous chapter, encrypted network applications can be identified based on TLS matches. However, if you are attempting to identify a network application that is already encrypted, such as Facebook Chat, decryption is necessary.

14.2 Key Concepts

- TLS Server Protection
- TLS Client Protection
- TLS Inspection Configuration
- Decryption Exceptions

14.3 TLS Server Protection

Server side decryption refers to traffic that is coming from the Internet to your server over HTTPS. The following are the basic steps of TLS Server Protection:

1. The server's certificate is imported into the SMC and made available to the NGFW during a policy installation.
2. When the connection comes into the server, the NGFW uses the server's certificate to decrypt the traffic. Once decrypted, inspection occurs as usual.
3. The NGFW uses the certificate to re-encrypt the traffic before forwarding it.

For a visual example of TLS Server Protection, please refer to the Student Guide.

14.4 TLS Client Protection

This scenario is different than TLS Server Protection in that you are not in control of the certificate. In this context, we are referring to traffic that is destined to an HTTPS server outside of your environment. By decrypting client traffic, it is possible to find data exfiltration, users attacking other networks, or other malicious activity. Below are the characteristics of TLS Client Protection:

- When a client initiates an outbound TLS connection, the NGFW examines the certificate to see if it was signed by a valid CA. The SMC maintains a list of Valid Certificate Authorities, as well as a CRL.
- If it was signed by a trusted CA, then the firewall makes a substitute certificate which is signed by the Client Protection CA that is built into the SMC.
- If the server's certificate was not signed by a trusted CA, the NGFW makes a new self-signed certificate that will be used for the connection. This will generate a browser warning message. After this, the connection will proceed as normal, while being decrypted an inspected.

For a detailed example of how TLS inspection is configured, please refer to the Student Guide.

Remember the following

1. TLS inspection is possible for both client and server communication.
2. When traffic is decrypted, it can be combined with deep inspection or other services such URL categorization (ThreatSeeker).
3. TLS inspection must be enabled in the NGFW properties in the Add-Ons section.
4. Decryption is enabled in the Allow action options in an access rule.
5. It is possible to define exceptions for Decryption. This can be done by creating a list of domains to exclude from Decryption, or you can create specific rules to prevent specific domains from being decrypted.
6. Clustering the NGFW will improve TLS inspection performance.
7. TLS inspection is included in the base license.

Chapter 15

Multi-Layer Deployments

15.1 Summary

As we have seen throughout the System Engineer course, each role has its specific function. The Firewall/VPN role performs most of its work at Layer 3, while the Layer 2 Firewall and IPS roles operate mostly on Layer 2. However, there are times when combining some of the functionality is useful and economical. When used in the Firewall/VPN role, you can take advantage of both firewall and IPS functionality. For example, if you would like to provide segmentation in a network, while still performing routing, NAT, etc., then Layer 2 interfaces would be useful. As with the Layer 2 firewall and IPS roles, pairs of interfaces can be configured to allow traffic to move between segments with no NAT applied, while also being inspected - just as if there was an IPS in place.

15.2 Key Cpncepts

- IPS and Layer 2 Firewall Key Features
- FW/VPN and IPS Differences
- IPS and Layer 2 Firewall Deployment
- Multi-layer Deployment
- High-availability Setup

15.3 IPS and Layer 2 Firewall Key Features

It goes without saying that the main thing shared by these two roles is that they are operating at layer 2, and as such, they do not alter the traffic. In the case of NAT, the traffic has to be changed somehow between interfaces. In layer 2 scenarios, traffic arrives on one interface, leaves on the other, and is inspected in the process.

It is important to remember that each role has its own policy type. The IPS uses IPS policies, and the Layer 2 Firewall uses Layer 2 Firewall policies. Both of these policies reference an Inspection Policy when deep inspection is being performed. The IPS and Layer 2 firewall share the same level of deep inspection. In a sense, their capabilities lay in their differences.

15.4 FW/VPN, Layer 2 Firewall, and IPS Differences

To better understand how each role is different, the following provides a short summary:

- **Firewall/VPN Role**: in this role, anything that is not specifically allowed is discarded. Unless Layer 2 interfaces are used, the Firewall/VPN role does not use Ethernet Access Rules. Also in this mode, connection tracking is net to normal. Normal connection tracking ensures that the firewall sees the entire connection from the beginning. The interfaces are fail-closed.
- **Layer 2 Firewall Role**: access rules are used, like the Firewall/VPN role, to control traffic; just as with the Firewall/VPN role, what is not specifically allowed is discarded. The Layer 2 Firewall role does have Ethernet Access rules, which allow it to control layer 2 protocols and MAC addresses. Unlike the Firewall/VPN role, the Layer 2 Firewall has no routing, NATing, or other Layer 3 capabilities. The network interfaces are fail-closed.
- **IPS Role**: the approach of the IPS is simply to dedicate its time to inspecting traffic. Unlike the Layer 2 Firewall and Firewall/VPN roles, the IPS will allow anything unless specifically discarded. In this way, you can use access control in the IPS policy to drop or allow things that should not be deep inspected. The IPS has no layer 3 functionality, except for the management, or control, interface. The interfaces are fail-open.

For additional detail, please refer to the Student Guide.

15.5 IPS and Layer 2 Firewall Deployment

Generally speaking, the IPS and Layer 2 Firewall have two ways they can be deployed - **inline** and out-of-line. When installed in-line, the Layer 2 Firewall or IPS has complete control over the traffic, in that they can terminate traffic directly if it violates the security policy. Traffic flows in one interface and out the other, thereby having to traverse the IPS or Layer 2 Firewall.

When the IPS or Layer 2 Firewall is connected to the span or mirror ports of a witch, where the traffic does not flow through it, it is said to be in **IDS** or Capture mode. In this mode (which really isn't a "mode" per se - just a matter of cabling), the NGFW cannot directly terminate the traffic. It can, however, send a TCP reset or request a blacklist from some other Forcepoint NGFW.

In some cases, it is valuable to mix these two "modes". This **hybrid** mode allows you to terminate terminate traffic on one pair of in-line interfaces, and listen on another interface. A use case would be to monitor traffic in another network that does not traverse the NGFW.

15.6 Multi-Layer Deployment

One of the great advantages of a Multi-layer deployment is that you can combine the features of the IPS and the Firewall/VPN role together in one appliance. This deployment allows you to perform all Firewall/VPN functions (e.g. routing, NAT, VPN) on some interfaces and perform IPS/Layer 2 Firewall functions on another set of interfaces. Layer 2 Interface policies control how traffic is handled with Layer 2 interfaces. The following is how traffic is handled by default for each interface type:

- **Inline Layer 2 Interface**:
  - Default Action for Access Control: DENY
  - Content Inspection: According to the Inspection Policy used
  - Failure Behavior: Fail-closed
- **Inline IPS Interface**:
  - Default Action for Access Control: ALLOW
  - Content Inspection: According to the Inspection Policy used
  - Failure Behavior: Fail-open
- **Capture Interface**:
  - Default Action for Access Control: ALLOW
  - Content Inspection: According to the Inspection Policy used

  - Failure Behavior: Fail-open

Please refer to the Student Guide for a visual representation of how to configure Layer 2 Interfaces in the Firewall/VPN role.

Remember the following

1. In Layer 2 Firewall or IPS roles, the NGFW will always have one interface that has an IP address on it. This is the Control Interface and is used for communicating with the SMC.
2. A Capture interface is an interface used in the IPS, Layer 2 Firewall, and Firewall/VPN modes (in the Firewall/VPN mode, Capture interfaces are only available when Layer 2 interfaces are configured.) The Capture interface has no IP address, is set to promiscuous mode, and is typically connected to the span or mirror port of a switch.
3. Using Layer 2 Interfaces in the Firewall/VPN role does not require a separate license.
4. Connection tracking in the Firewall/VPN and Layer 2 Firewall roles is set to normal.
5. Connection tracking in the IPS role is set to loose.
6. In the Firewall/VPN and Layer
7. When the IPS is used as an IDS (meaning that it isn't in the path of the traffic), it does not have direct control over the connection. In order to stop something malicious, the IPS can send a reset packet or have the connection blacklisted by some other Forcepoint NGFW.
8. NGFWs in the IPS role can be clustered to form a Serial IPS cluster, offering High Availability for deep inspection. Please refer to the Student Guide for additional details.
9. NGFWs in Layer 2 Firewall mode can be clustered. Only Active-Standby clustering is supported.
10. When an NGFW is operating in the Firewall/VPN mode and using in-line Layer 2 interfaces, only Active-Standby is supported.
11. When an NGFW is operating in the Firewall/VPN rile and using in-line IPS interfaces, Active-Active clustering is supported.
12. In order to use the fail-open feature of in-line interfaces, the appliance must have an interface module that supports fail-open.
13. Fail-open interfaces allow all traffic through (at a hardware level) - useful in situations where the network must remain up regardless of software or hardware failure.

Chapter 16

Forcepoint Security Integrations