Network Security Controls - Technical Controls

Exercise 1: Implementing Host-Based Firewall Protection with iptables

Iptables is a command-line firewall utility that uses policy chains to allow or block traffic.

Lab Scenario

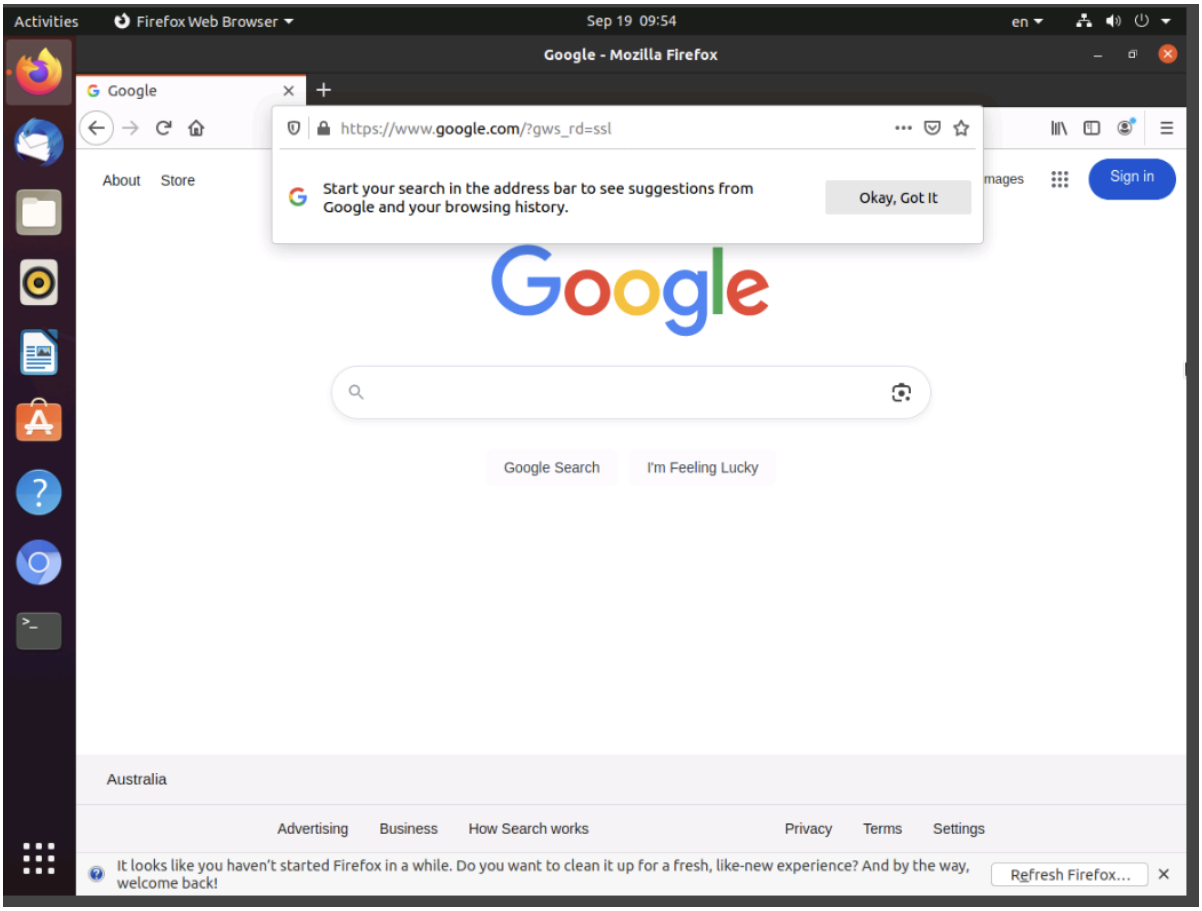
As a network defender, you should know how to configure an iptables host-based firewall to allow or block traffic to or from a Linux system. Iptables allow network defenders to enter firewall rules into the existing tables using the command line.

Lab Objectives

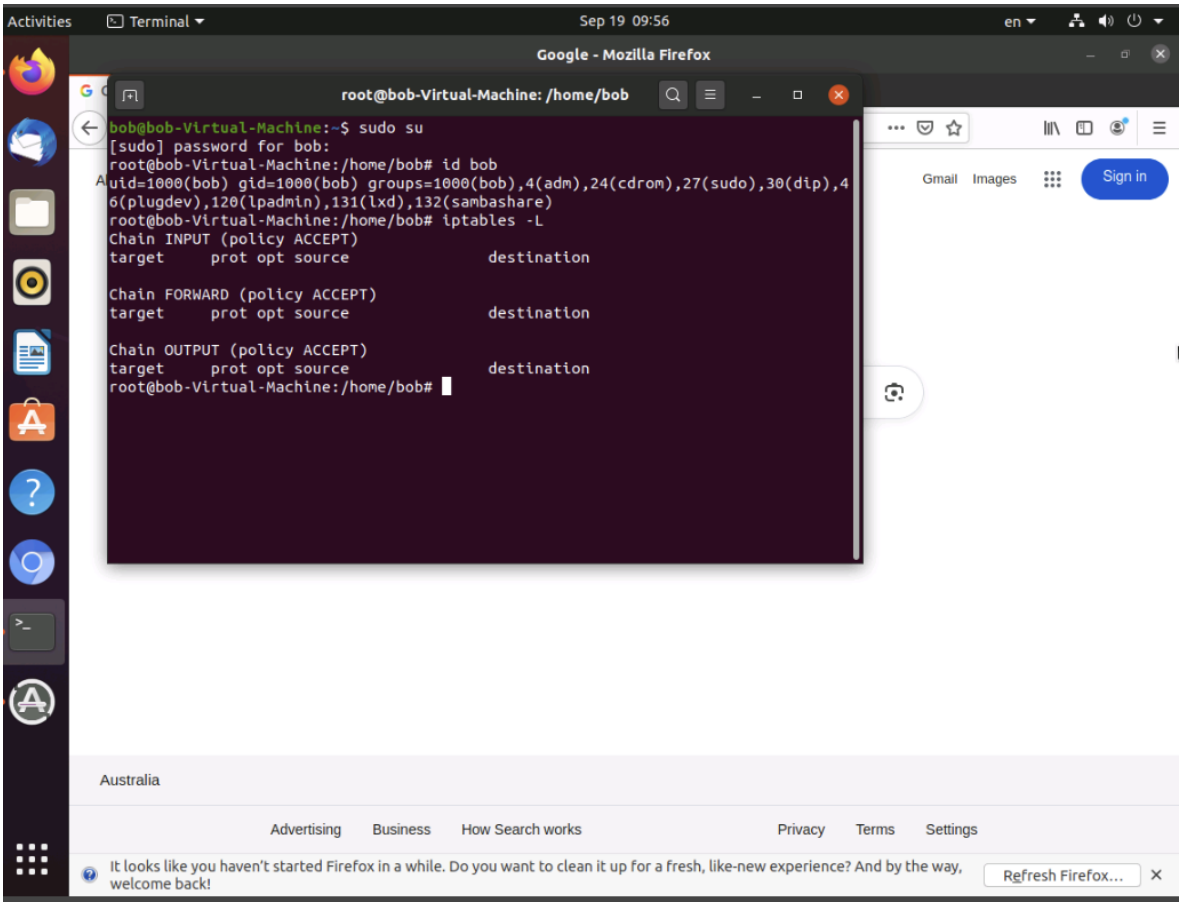
This lab will demonstrate how to configure an iptables host-based firewall in an Ubuntu machine.

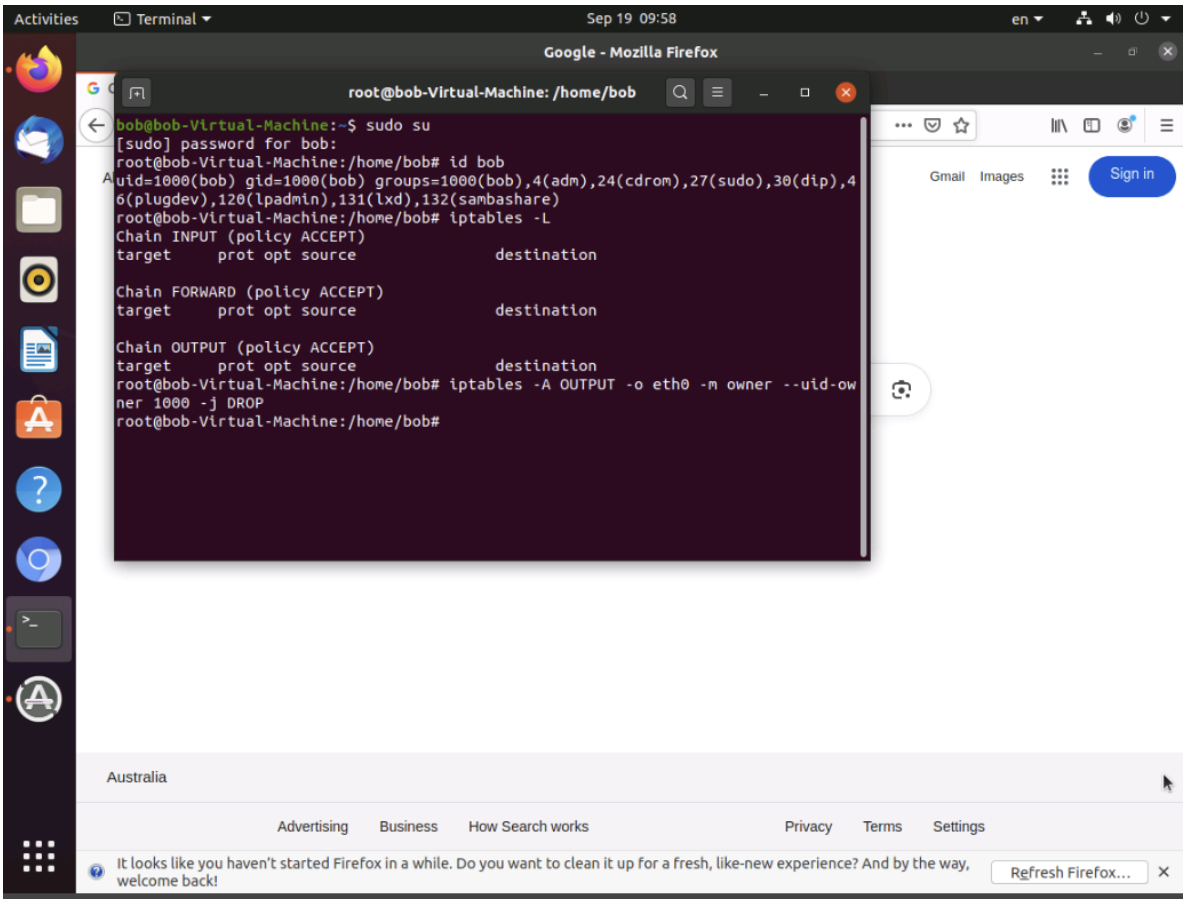
Overview of iptables

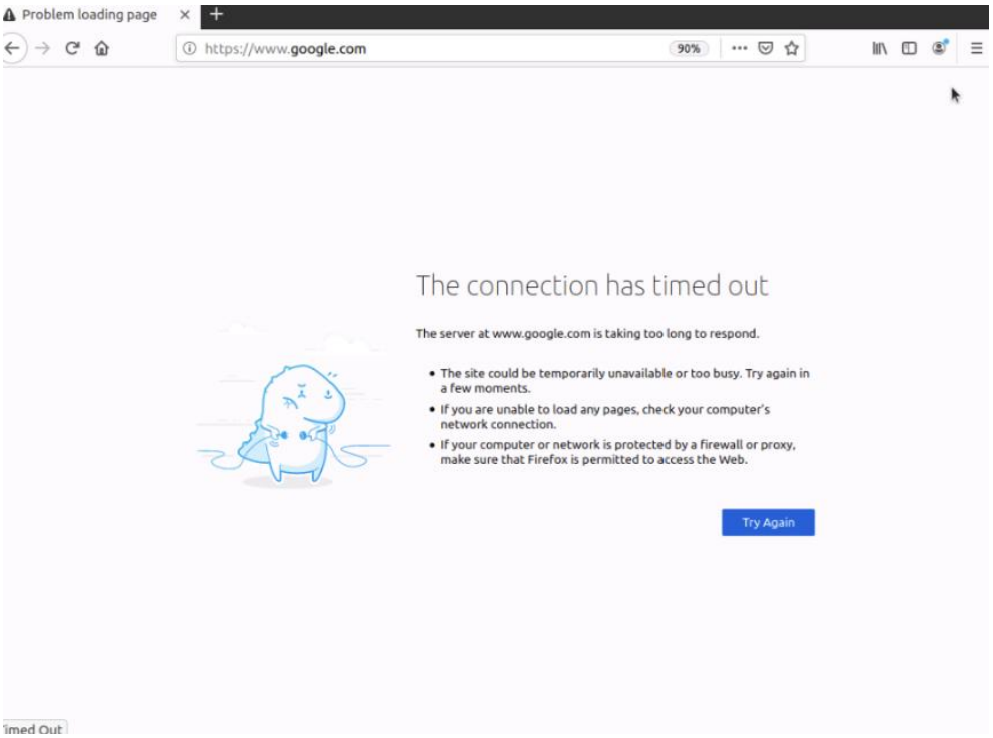
iptables is a standard firewall included in most Linux distributions. With the default chain policies configured, you can start adding rules to iptables, so that it knows what to do when it encounters a connection from or to a particular IP address or port.

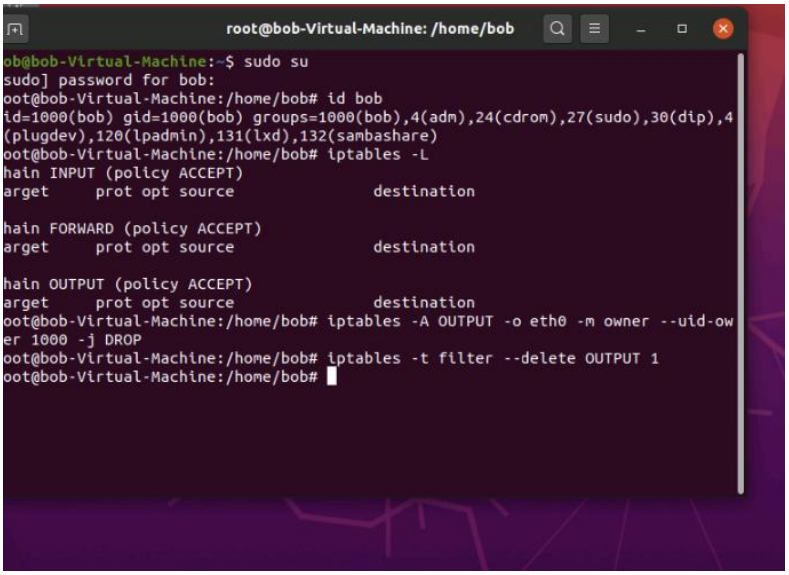


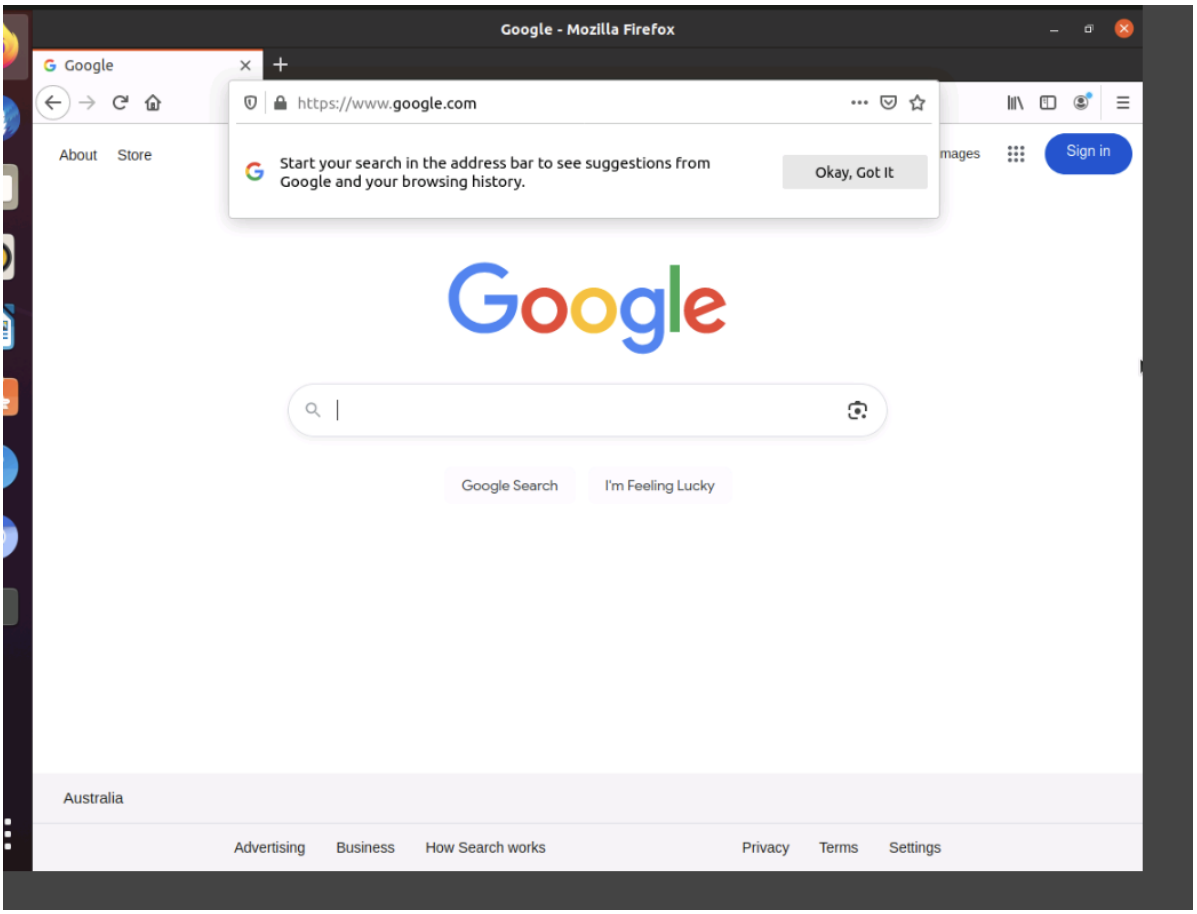
Bob is able to access the website, which implies that Bob has internet access. A network defender can block internet access on the user machine using iptables.




Activities
Terminal
Sep 19 09:58
en
Google - Mozilla Firefox
root@bob-Virtual-Machine: /home/bob
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# id bob
uid=1000(bob) gid=1000(bob) groups=1000(bob),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
root@bob-Virtual-Machine:/home/bob# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@bob-Virtual-Machine:/home/bob# iptables -A OUTPUT -o eth0 -m owner --uid-owner 1000 -j DROP
root@bob-Virtual-Machine:/home/bob#
Gmail
Images
Sign in
Australia
Advertising
Business
How Search works
Privacy
Terms
Settings
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...


Problem loading page
https://www.google.com
90%
The connection has timed out
The server at www.google.com is taking too long to respond.
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.
Try Again





Exercise 2: Implementing Host-Based Firewall Functionality using Windows Firewall

A host-based firewall protects the system from various threats. Configuring a host-based firewall will help achieve the real security implementation and Defense in Depth within an organization. The normal strategy of a host-based firewall is to provide defense-in-depth and use a combination of layers of protection within the organization.

Lab Scenario

Network defenders implemented various security layers in the organization; a single breach in security can allow the attacker to leave malicious code or transfer the malicious file over the network. Host-based firewall implementation is another security layer where the admin can allow or restrict specific individual endpoints. In this lab, you will configure a host-based firewall to protect the individual system connected to the network.

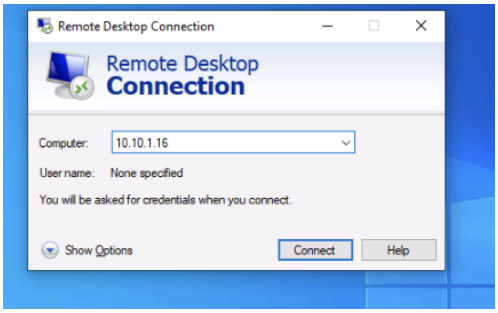
Lab Objectives

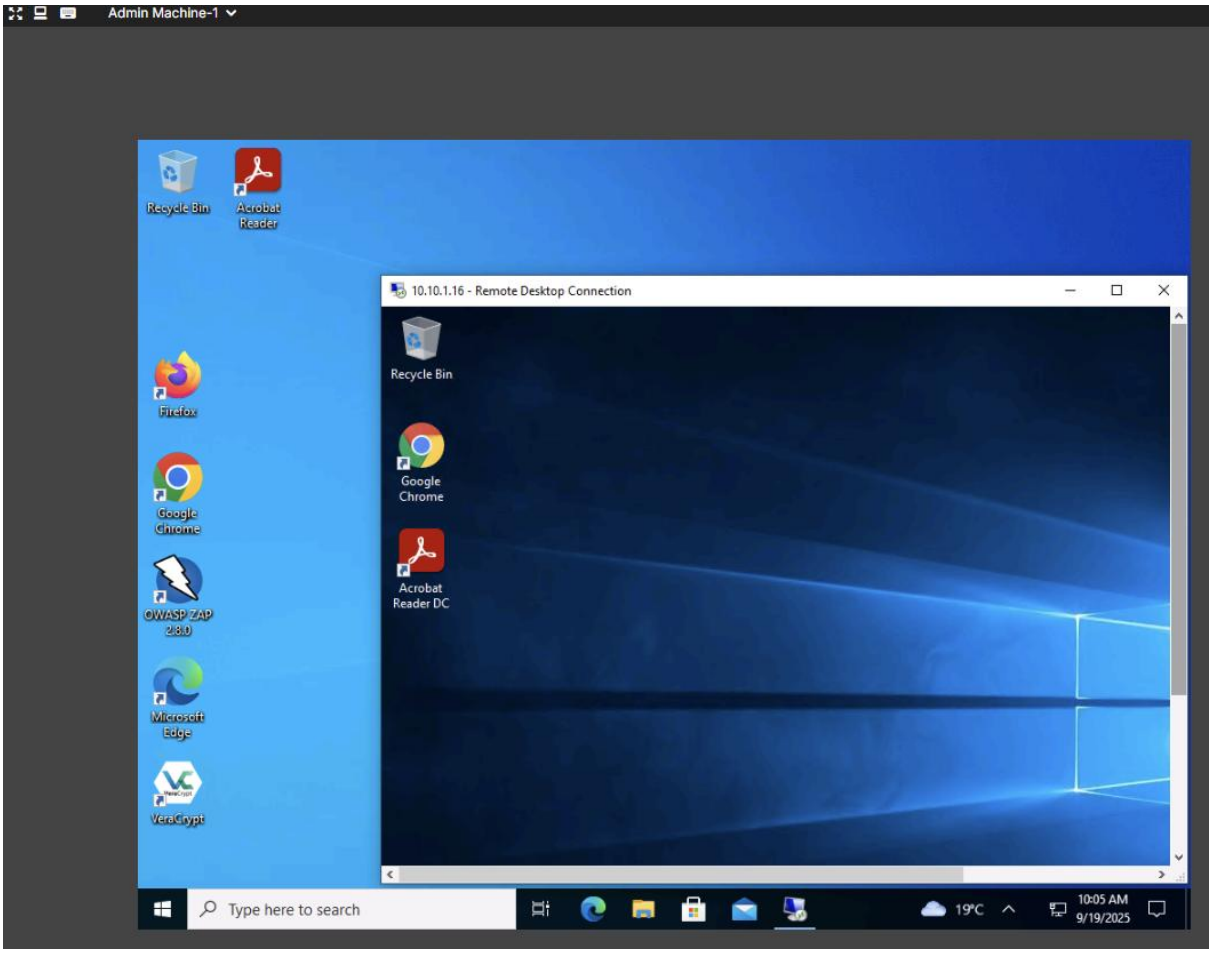
This lab will demonstrate how to secure an individual endpoint within the network. In this lab, you will learn how to do the following:

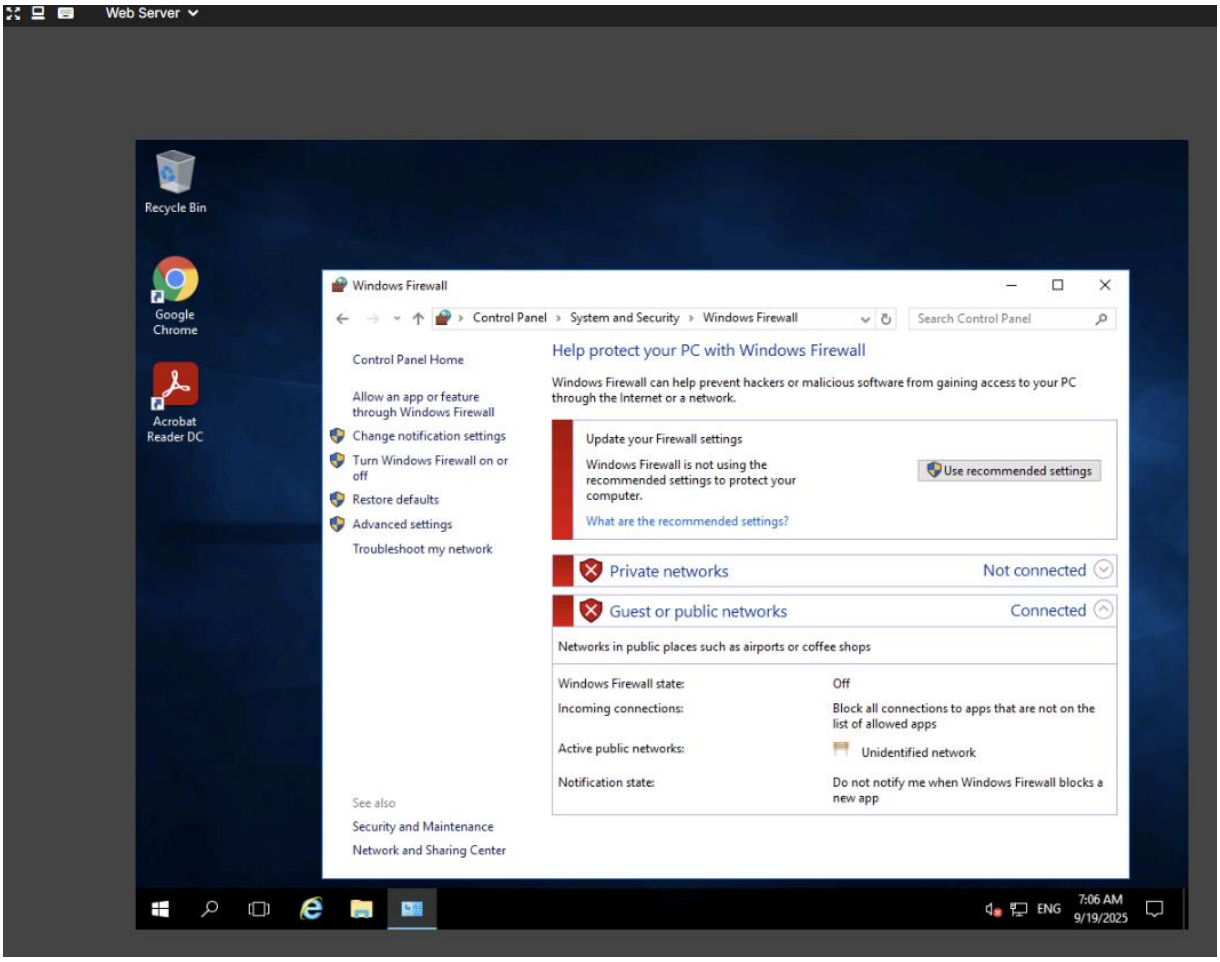
- Hardening the host within the network
- Applying rules in a host-based firewall

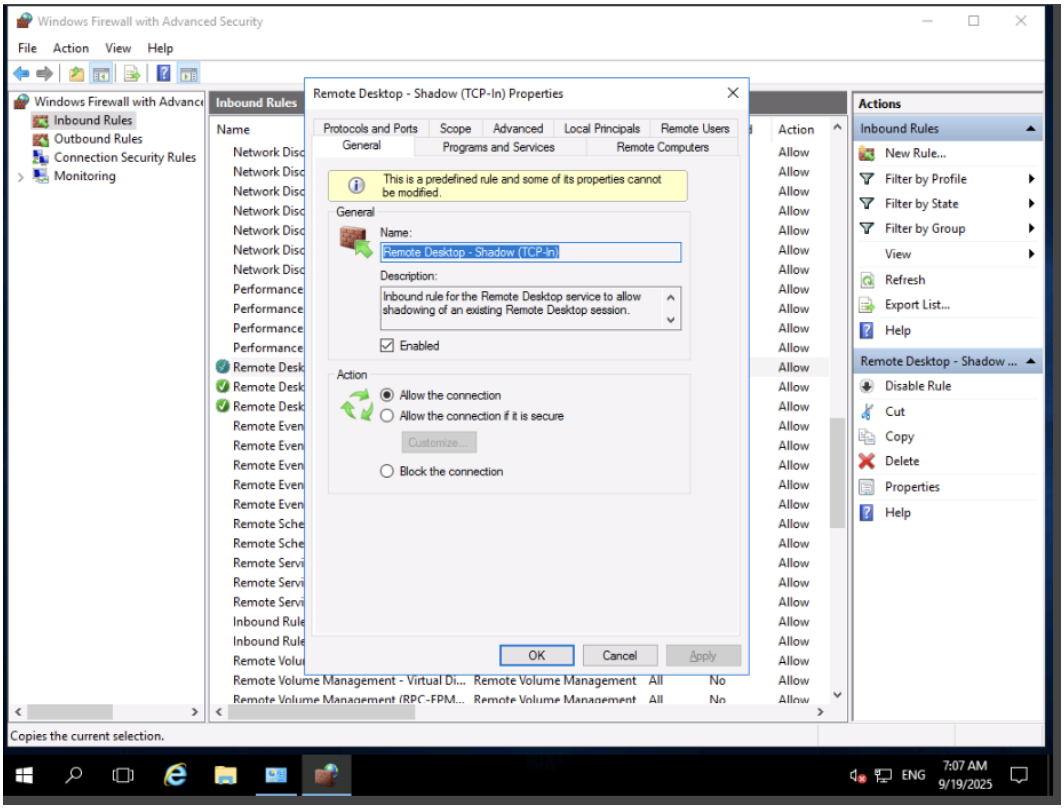
Overview of a Host-based Firewall

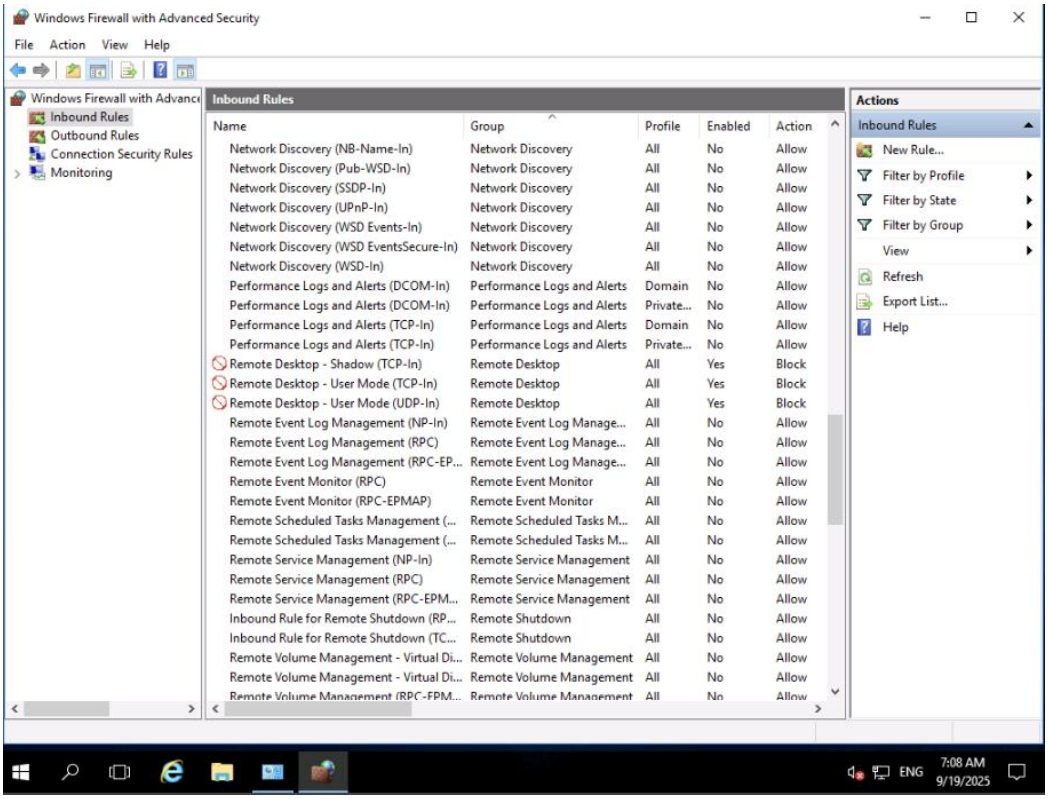
A host-based firewall is a software that makes the system or device secure. An example is the Windows firewall, which is inbuilt in the Windows platform. The Windows firewall developed by Microsoft Windows is an application that filters the incoming and outgoing Internet traffic and blocks the malicious program communicating to the individual endpoint. The Windows firewall (host-based) protects the individual endpoint over the network from various threats, viruses, and malware.

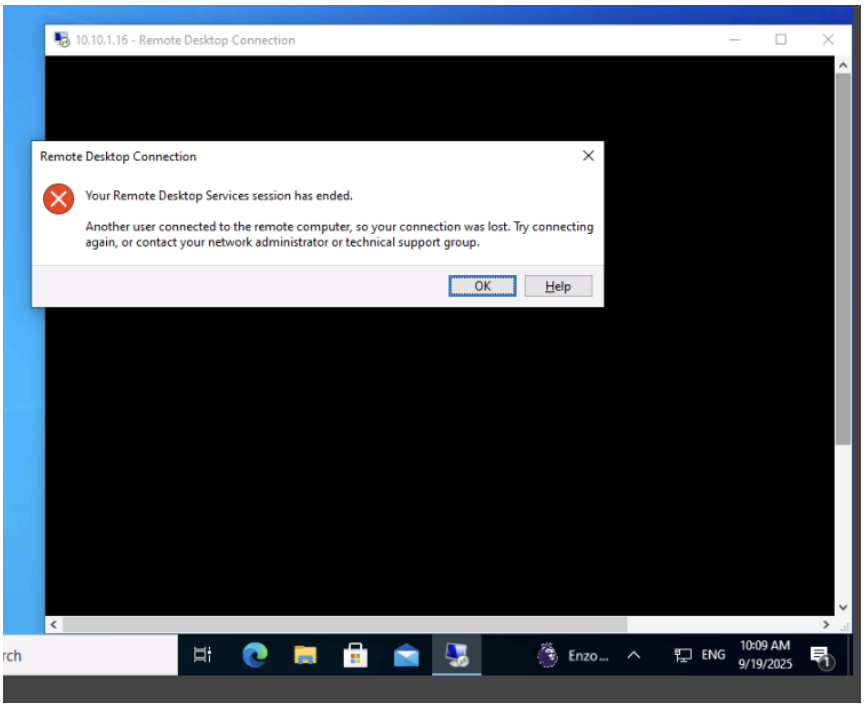



Admin Machine-1
Recycle Bin
Acrobat Reader
Firefox
Google Chrome
OWASP ZAP 2.8.0
Microsoft Edge
VeraCrypt
10.10.1.16 - Remote Desktop Connection
Recycle Bin
Google Chrome
Acrobat Reader DC
Type here to search
19°C
10:05 AM
9/19/2025

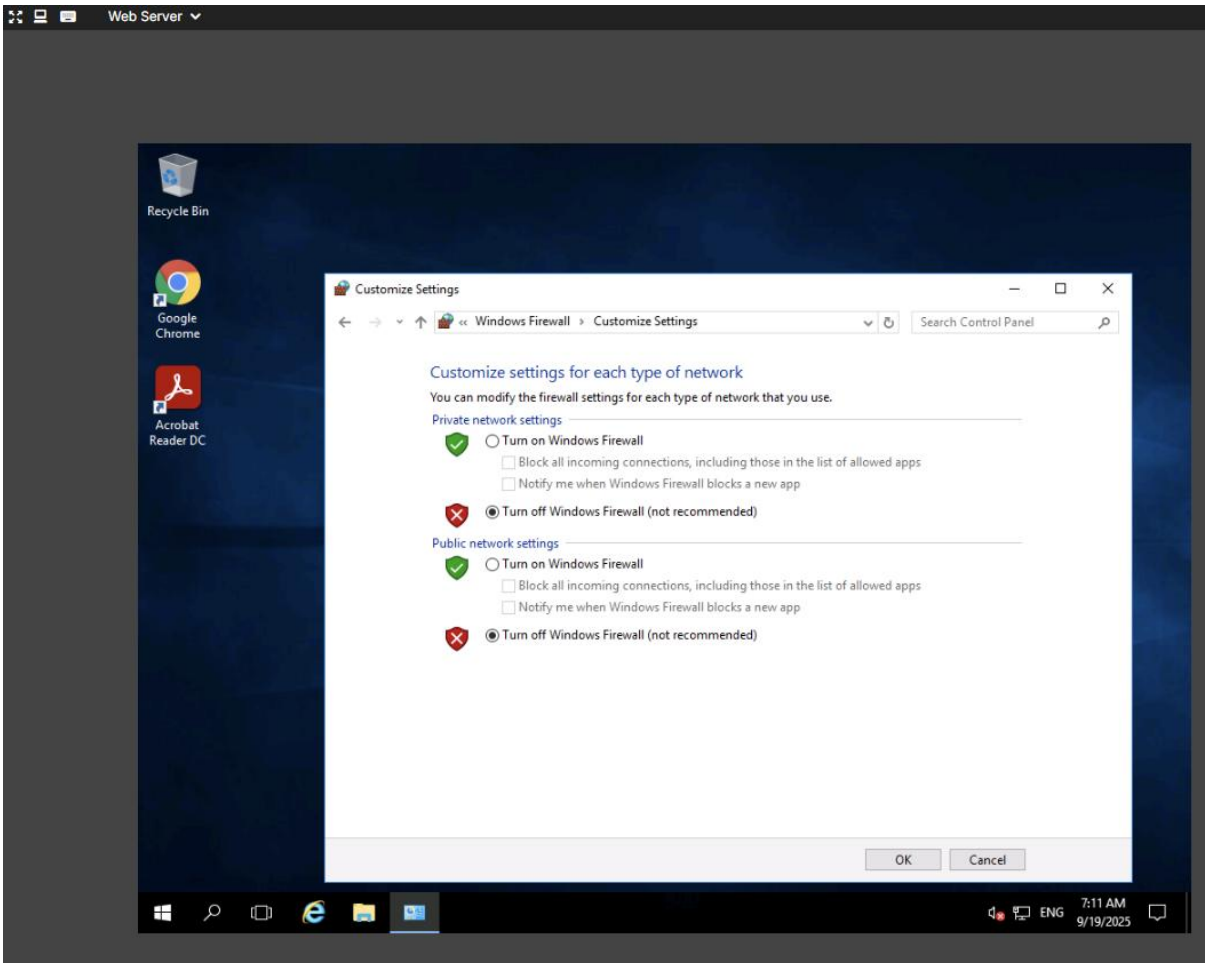

Web Server
Recycle Bin
Google Chrome
Acrobat Reader DC
Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Update your Firewall settings
Windows Firewall is not using the recommended settings to protect your computer.
Use recommended settings
What are the recommended settings?
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state:
Off
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
Unidentified network
Notification state:
Do not notify me when Windows Firewall blocks a new app
See also
Security and Maintenance
Network and Sharing Center
ENG
7:06 AM
9/19/2025

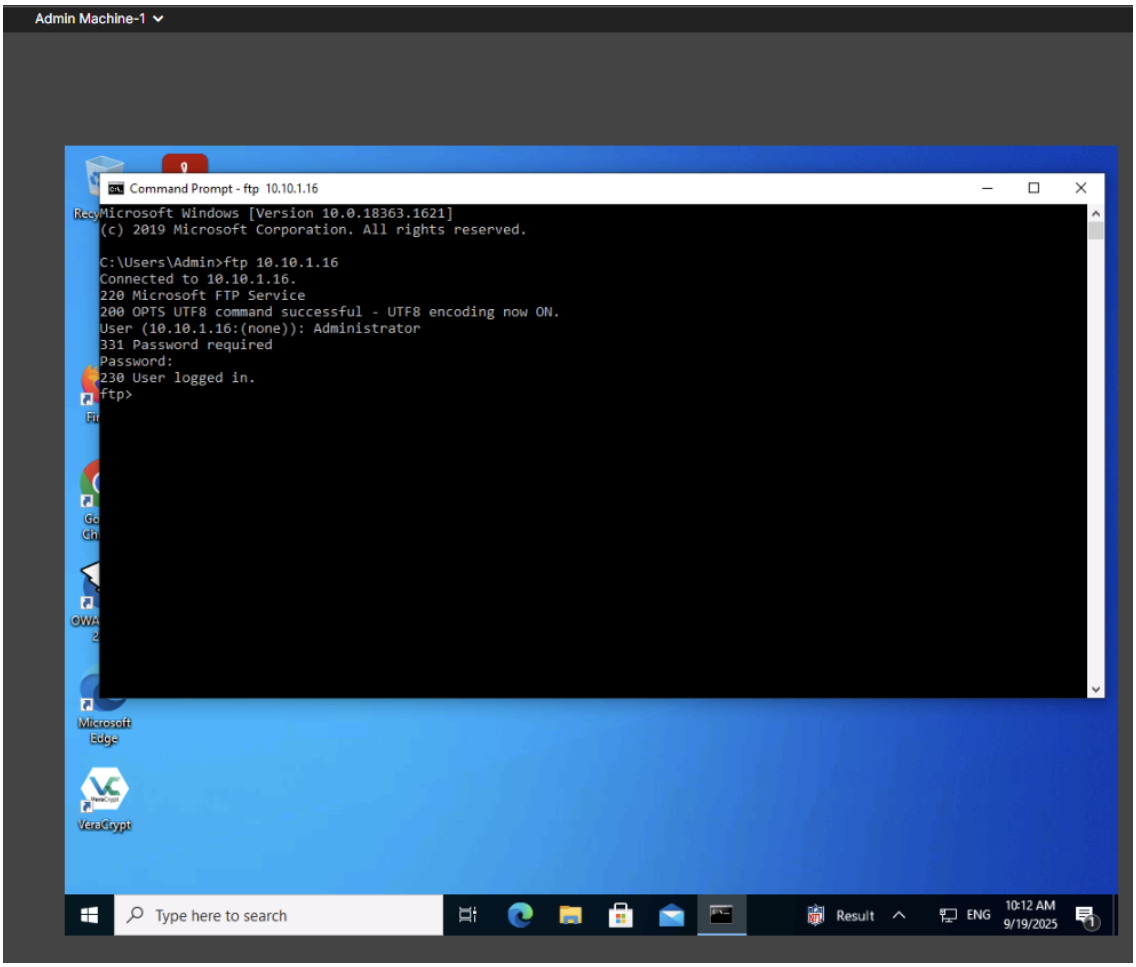

Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Action
Remote Desktop - Shadow (TCP-In) Properties
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
General
Programs and Services
Remote Computers
This is a predefined rule and some of its properties cannot be modified.
General
Name:
Remote Desktop - Shadow (TCP-In)
Description:
Inbound rule for the Remote Desktop service to allow shadowing of an existing Remote Desktop session.
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
OK
Cancel
Apply
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Remote Desktop - Shadow ...
Disable Rule
Cut
Copy
Delete
Properties
Help
Copies the current selection.
ENG
7:07 AM
9/19/2025

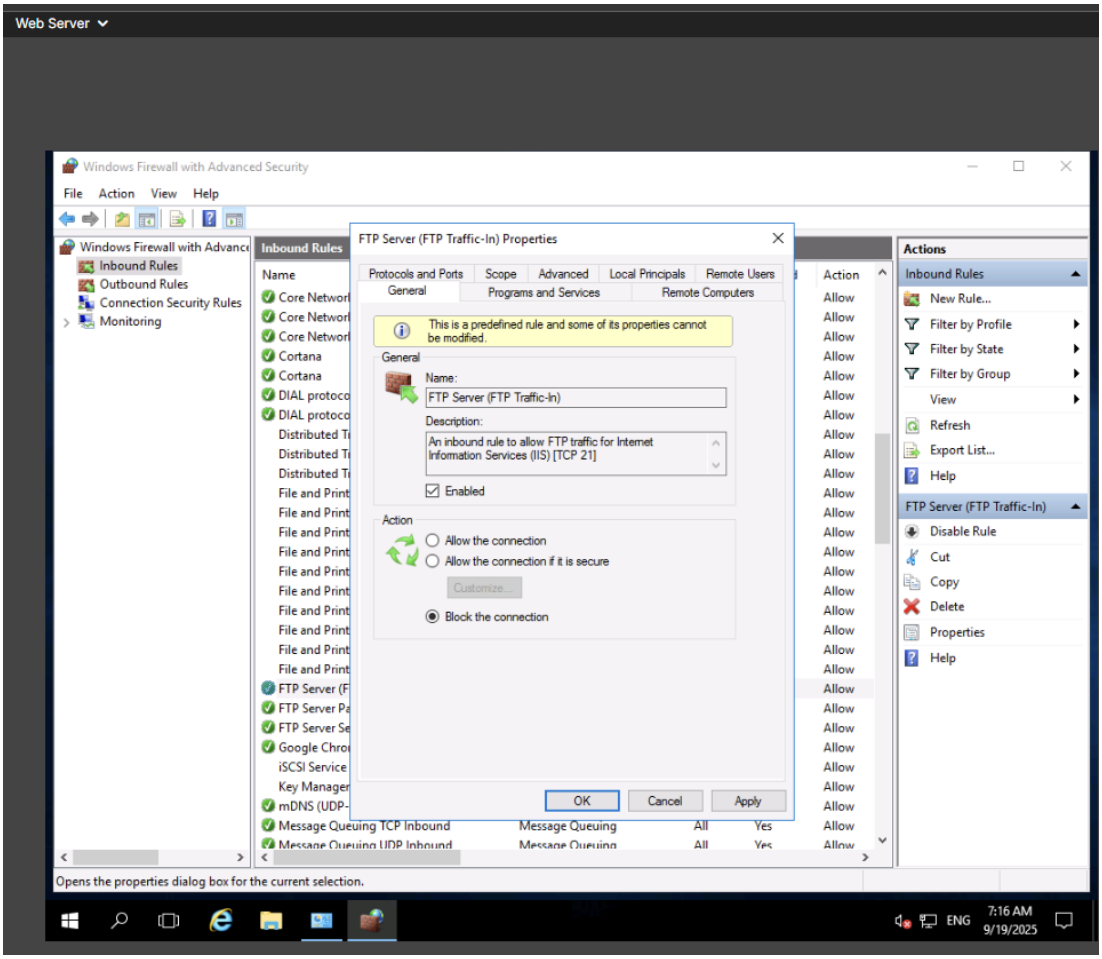

Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Network Discovery (NB-Name-In) Network Discovery All No Allow
Network Discovery (Pub-WSD-In) Network Discovery All No Allow
Network Discovery (SSDP-In) Network Discovery All No Allow
Network Discovery (UPnP-In) Network Discovery All No Allow
Network Discovery (WSD Events-In) Network Discovery All No Allow
Network Discovery (WSD EventsSecure-In) Network Discovery All No Allow
Network Discovery (WSD-In) Network Discovery All No Allow
Performance Logs and Alerts (DCOM-In) Performance Logs and Alerts Domain No Allow
Performance Logs and Alerts (DCOM-In) Performance Logs and Alerts Private... No Allow
Performance Logs and Alerts (TCP-In) Performance Logs and Alerts Domain No Allow
Performance Logs and Alerts (TCP-In) Performance Logs and Alerts Private... No Allow
Remote Desktop - Shadow (TCP-In) Remote Desktop All Yes Block
Remote Desktop - User Mode (TCP-In) Remote Desktop All Yes Block
Remote Desktop - User Mode (UDP-In) Remote Desktop All Yes Block
Remote Event Log Management (NP-In) Remote Event Log Manage... All No Allow
Remote Event Log Management (RPC) Remote Event Log Manage... All No Allow
Remote Event Log Management (RPC-EP... Remote Event Log Manage... All No Allow
Remote Event Monitor (RPC) Remote Event Monitor All No Allow
Remote Event Monitor (RPC-EPMAP) Remote Event Monitor All No Allow
Remote Scheduled Tasks Management (... Remote Scheduled Tasks M... All No Allow
Remote Scheduled Tasks Management (... Remote Scheduled Tasks M... All No Allow
Remote Service Management (NP-In) Remote Service Management All No Allow
Remote Service Management (RPC) Remote Service Management All No Allow
Remote Service Management (RPC-EPM... Remote Service Management All No Allow
Inbound Rule for Remote Shutdown (RP... Remote Shutdown All No Allow
Inbound Rule for Remote Shutdown (TC... Remote Shutdown All No Allow
Remote Volume Management - Virtual Di... Remote Volume Management All No Allow
Remote Volume Management - Virtual Di... Remote Volume Management All No Allow
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
ENG
7:08 AM
9/19/2025

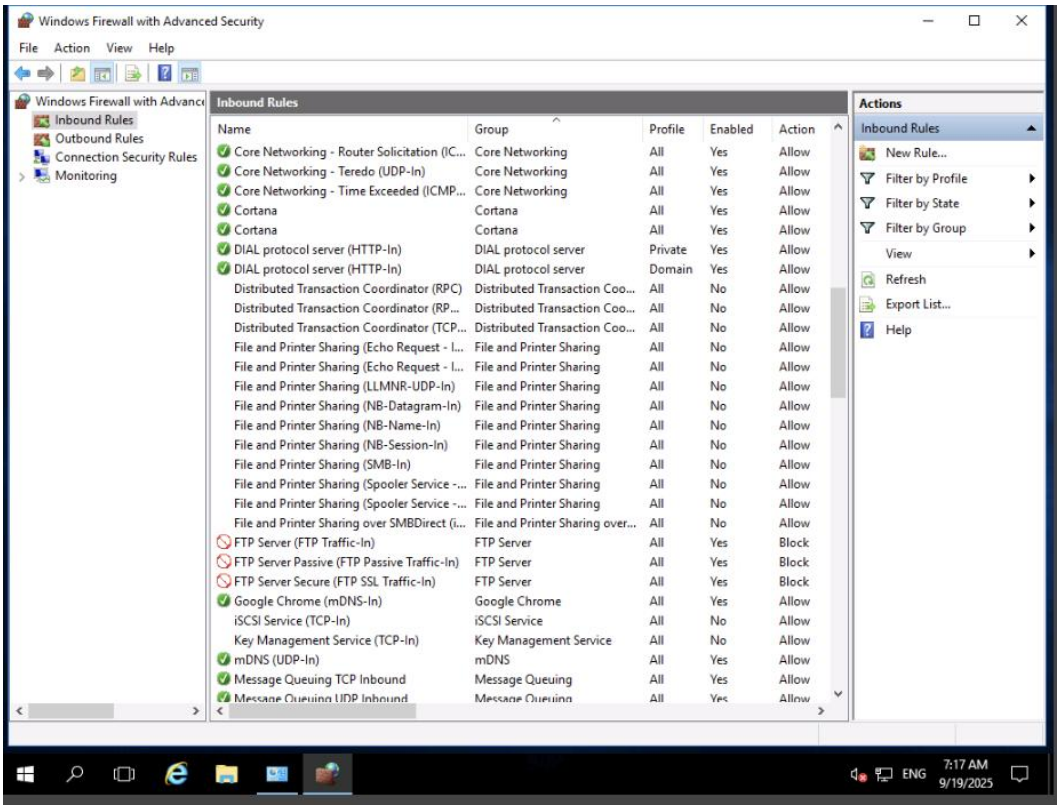

10.10.1.16 - Remote Desktop Connection
Remote Desktop Connection
Your Remote Desktop Services session has ended.
Another user connected to the remote computer, so your connection was lost. Try connecting again, or contact your network administrator or technical support group.
OK
Help
ENG
10:09 AM
9/19/2025

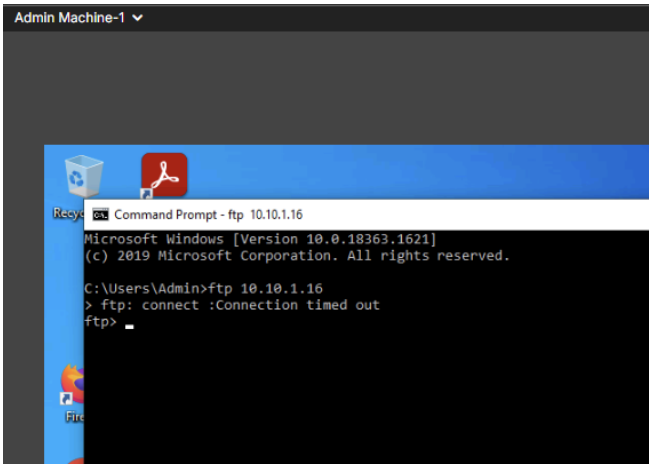

Remote Desktop Connection
Remote Desktop Connection
Remote Desktop Connection
Remote Desktop can't connect to the remote computer for one of these reasons:
1) Remote access to the server is not enabled
2) The remote computer is turned off
3) The remote computer is not available on the network
Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.
OK
Help


Web Server
Recycle Bin
Google Chrome
Acrobat Reader DC
Customize Settings
« Windows Firewall › Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Private network settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Firewall blocks a new app
Turn off Windows Firewall (not recommended)
Public network settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Firewall blocks a new app
Turn off Windows Firewall (not recommended)
OK
Cancel
ENG
7:11 AM
9/19/2025


Admin Machine-1
Command Prompt - ftp 10.10.1.16
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Admin>ftp 10.10.1.16
Connected to 10.10.1.16.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.10.1.16:(none)): Administrator
331 Password required
Password:
230 User logged in.
ftp>
Microsoft Edge
VeraCrypt
Type here to search
Result
ENG
10:12 AM
9/19/2025


Web Server
Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Action
Core Networ
Cortana
DIAL protoco
Distributed Tr
File and Print
FTP Server (F
FTP Server Pa
FTP Server Se
Google Chro
iSCSI Service
Key Manager
mDNS (UDP-
Message Queuing TCP Inbound
Message Queuing UDP Inbound
Allow
Yes
FTP Server (FTP Traffic-In) Properties
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
General
Programs and Services
Remote Computers
This is a predefined rule and some of its properties cannot be modified.
General
Name:
FTP Server (FTP Traffic-In)
Description:
An inbound rule to allow FTP traffic for Internet Information Services (IIS) [TCP 21]
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
OK
Cancel
Apply
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
FTP Server (FTP Traffic-In)
Disable Rule
Cut
Copy
Delete
Properties
Help
Opens the properties dialog box for the current selection.
ENG
7:16 AM
9/19/2025





Exercise 3: Implementing Network-Based Firewall Functionality: Blocking Unwanted Website Access using pfSense Firewall

The pfSense firewall/router is the world's most trusted open-source network security solution software. A network defender can use the pfSense firewall to manage network security easily.

Lab Scenario

To prevent users from visiting malicious websites and to secure against phishing attacks, network defenders need to block known malicious websites and protect the network from various viruses and malware. As a security measure organizations to prevent employees from accessing unwanted websites for employees.

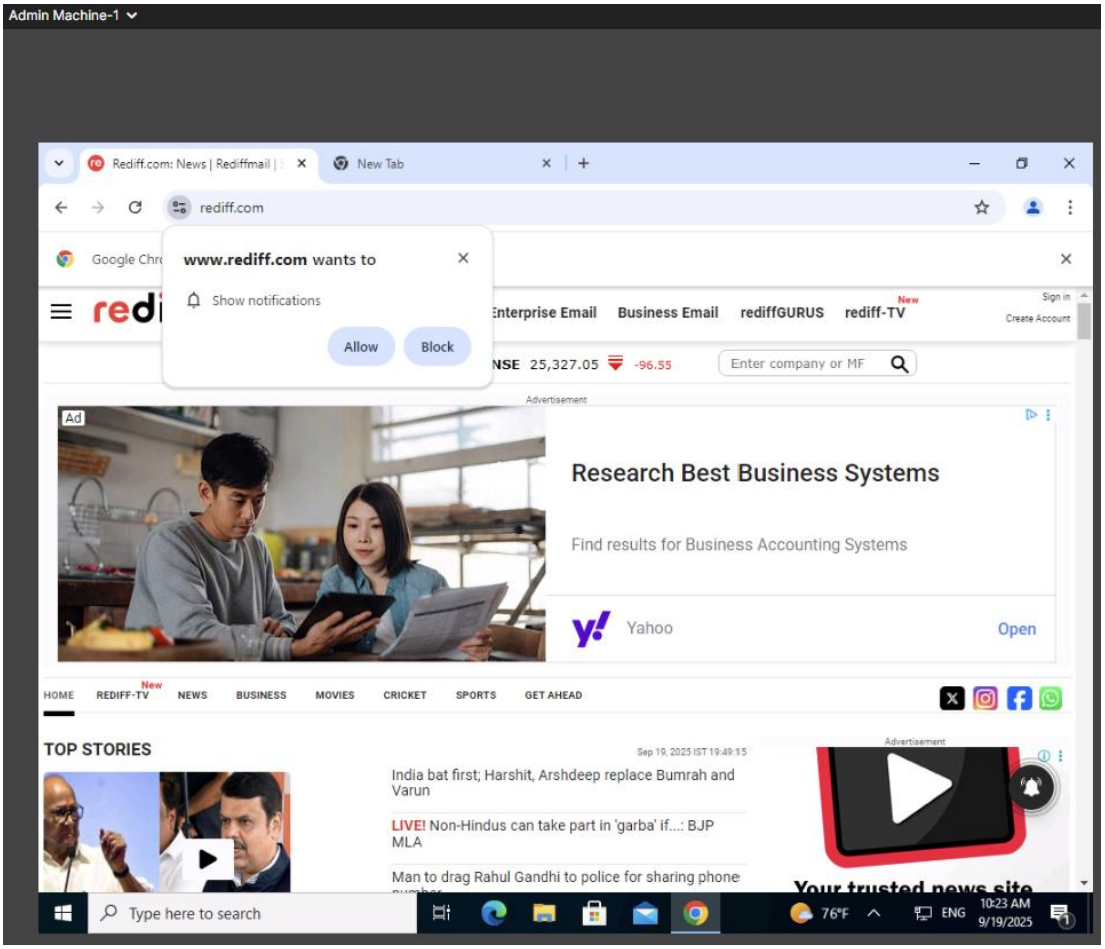
Lab Objectives

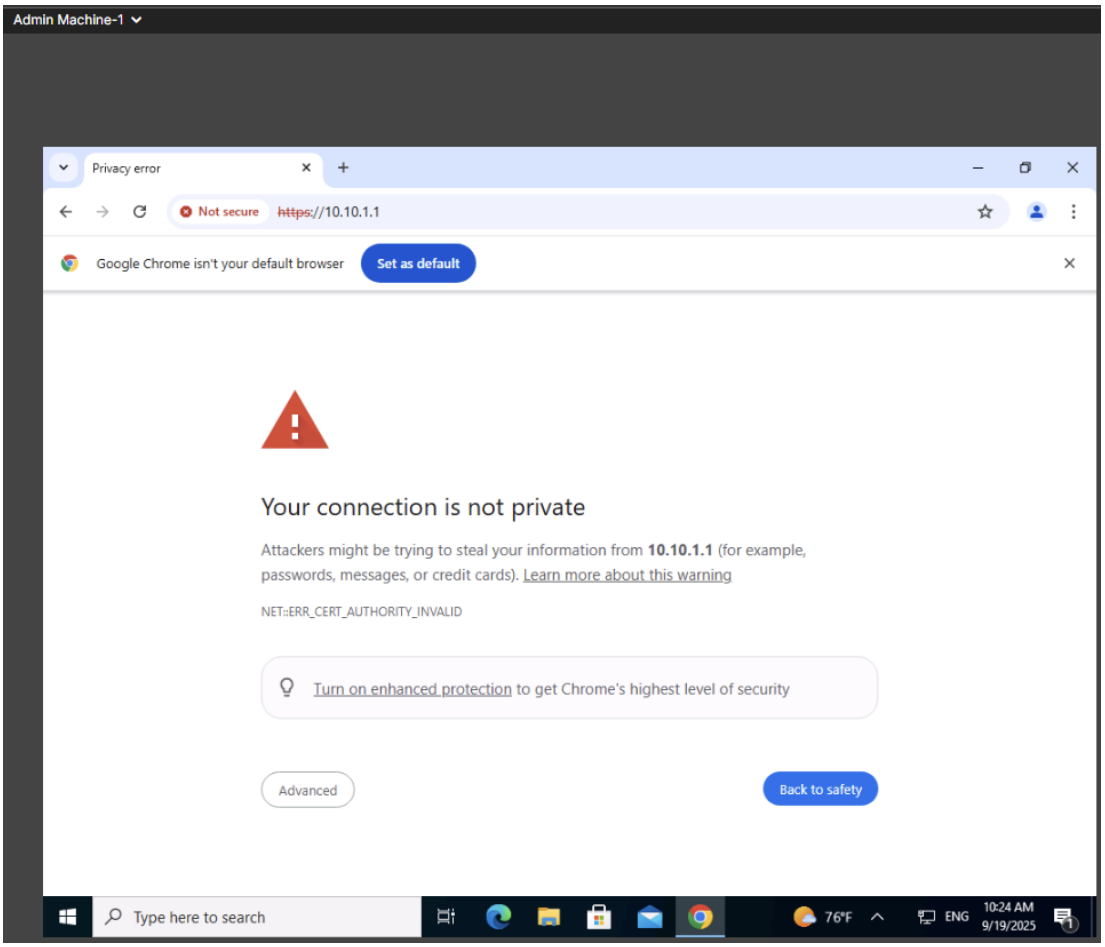
The lab will demonstrate how to use the pfSense firewall alias to block access to unwanted websites. If we implement one rule per host, the number of rules will be greater and more difficult to manage. Using an alias for multiple hosts requires the use of only one rule.

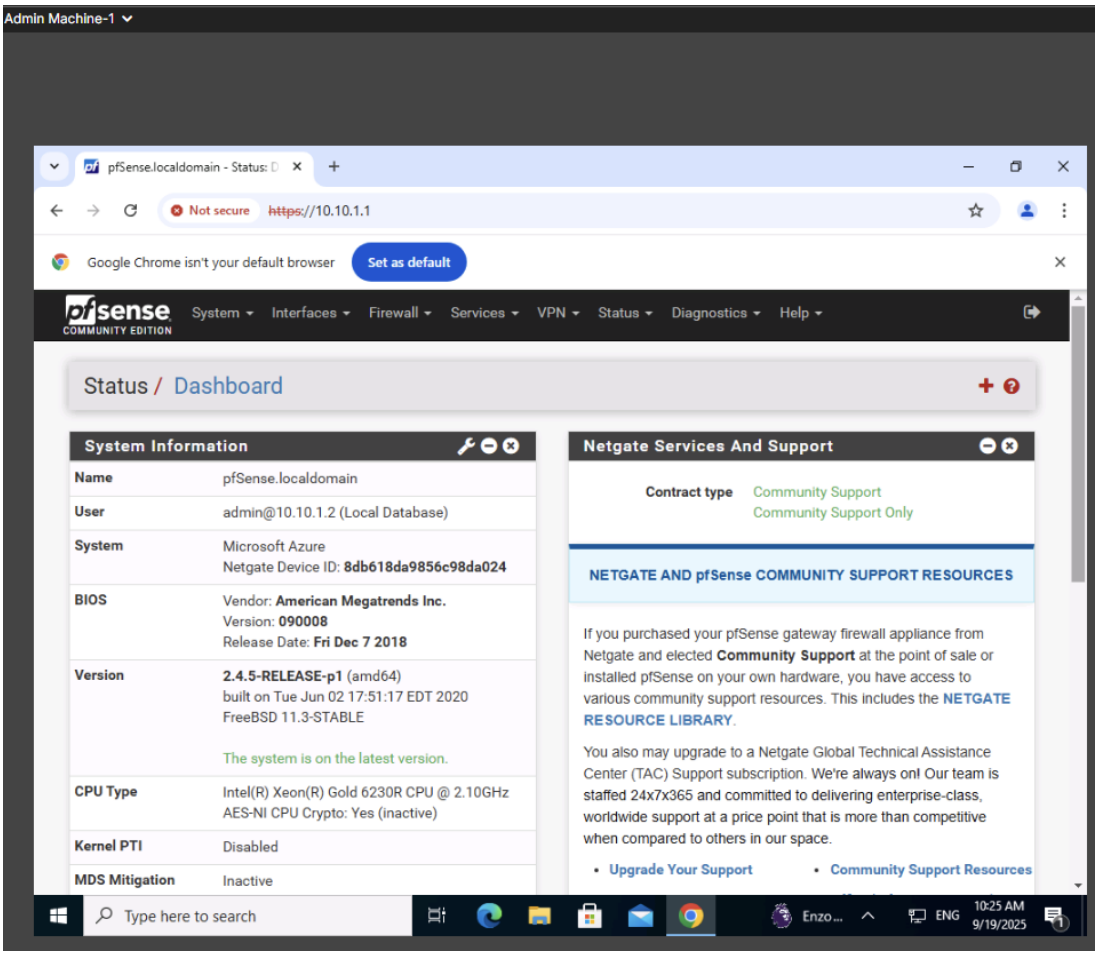
Overview of pfSense Firewall

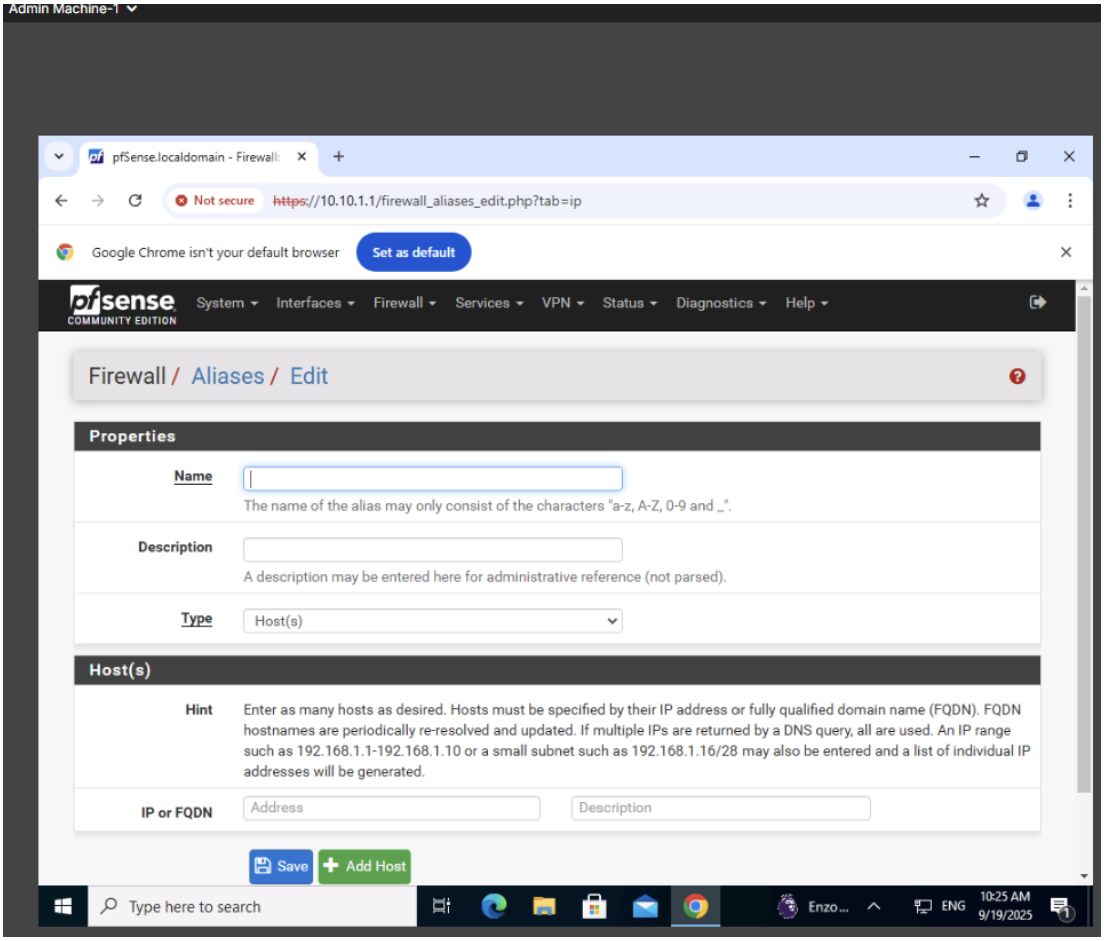
pfSense is a free, open-source Operating System that functions like a firewall, intrusion detection system, and router. Firewall features are integrated into pfSense, and it contains basic firewall rules and firewall logs.

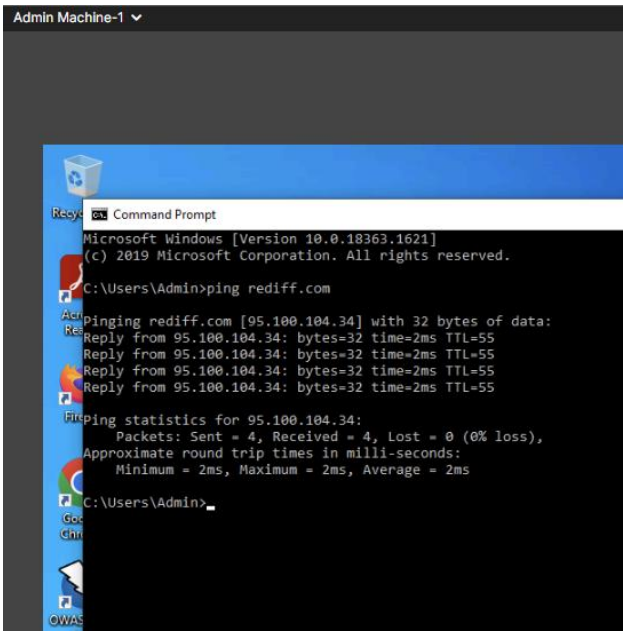
Aliases act as placeholders for real hosts, networks, or ports and help in reducing the number of changes required when the host, network, or port changes. The name of an alias can be used instead of specifying the host, network, or port for defining firewall rules.

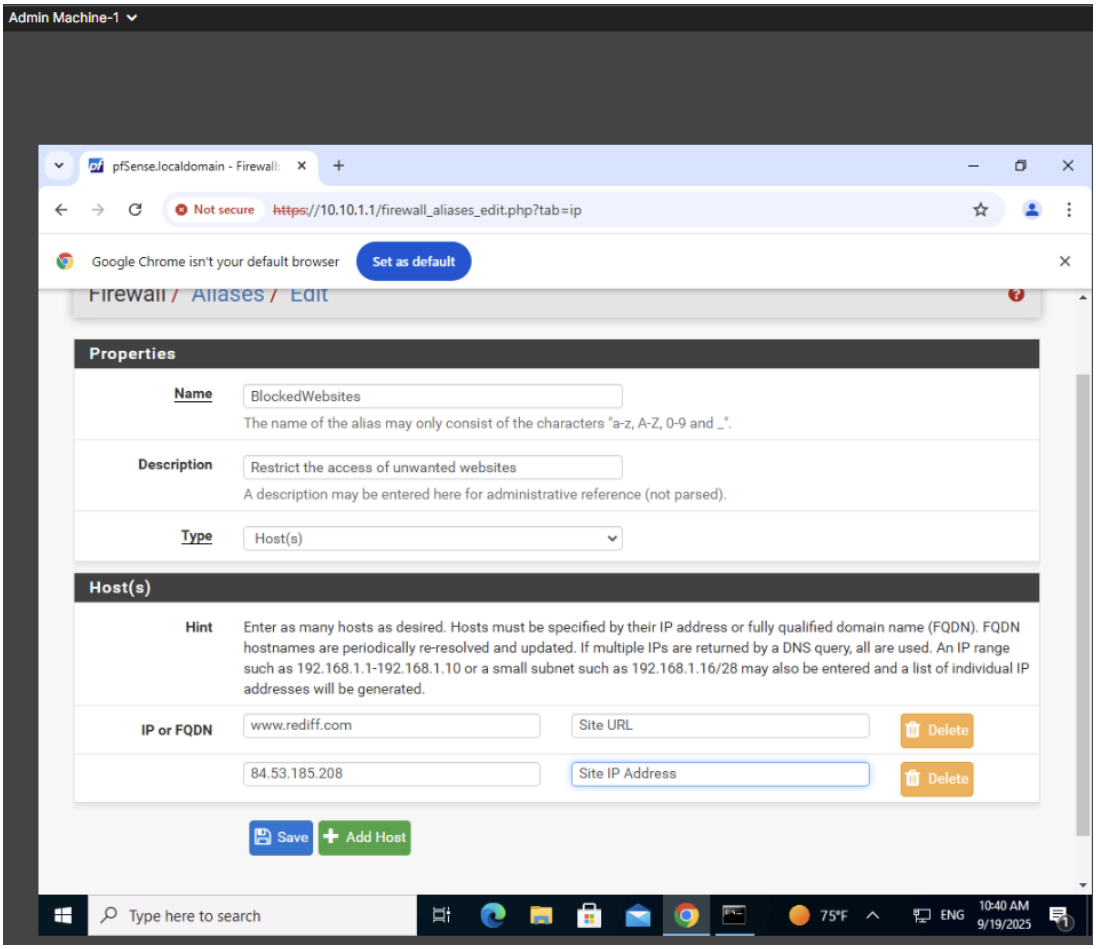

Admin Machine-1
Rediff.com: News | Rediffmail
New Tab
rediff.com
www.rediff.com wants to
Show notifications
Allow
Block
Enterprise Email
Business Email
rediffGURUS
rediff-TV
New
Sign in
Create Account
NSE 25,327.05 -96.55
Enter company or MF
Advertisement
Ad
Research Best Business Systems
Find results for Business Accounting Systems
Yahoo
Open
HOME
REDIFF-TV
New
NEWS
BUSINESS
MOVIES
CRICKET
SPORTS
GET AHEAD
TOP STORIES
Sep 19, 2025 IST 19:49:15
India bat first; Harshit, Arshdeep replace Bumrah and Varun
LIVE! Non-Hindus can take part in 'garba' if...: BJP MLA
Man to drag Rahul Gandhi to police for sharing phone
Advertisement
Your trusted news site
Type here to search
76°F
ENG
10:23 AM
9/19/2025

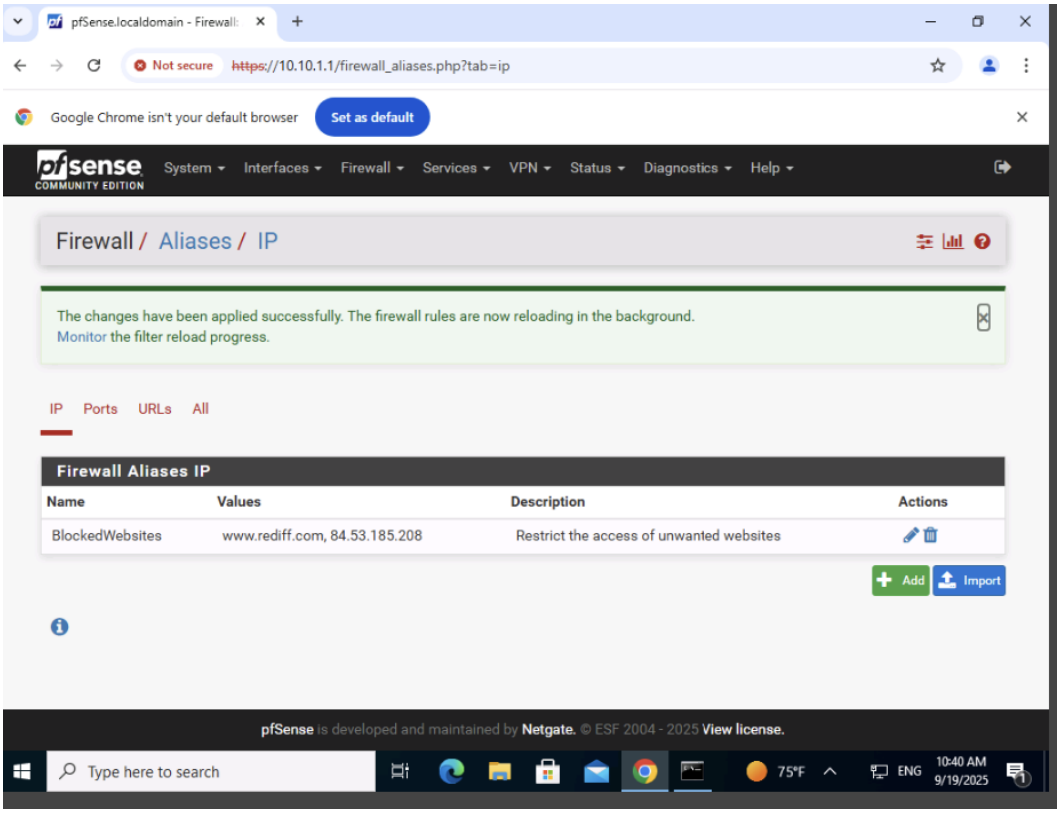

Admin Machine-1
Privacy error
Not secure
https://10.10.1.1
Google Chrome isn't your default browser
Set as default
Your connection is not private
Attackers might be trying to steal your information from 10.10.1.1 (for example, passwords, messages, or credit cards). Learn more about this warning
NET::ERR_CERT_AUTHORITY_INVALID
Turn on enhanced protection to get Chrome's highest level of security
Advanced
Back to safety
Type here to search
76°F
ENG
10:24 AM
9/19/2025

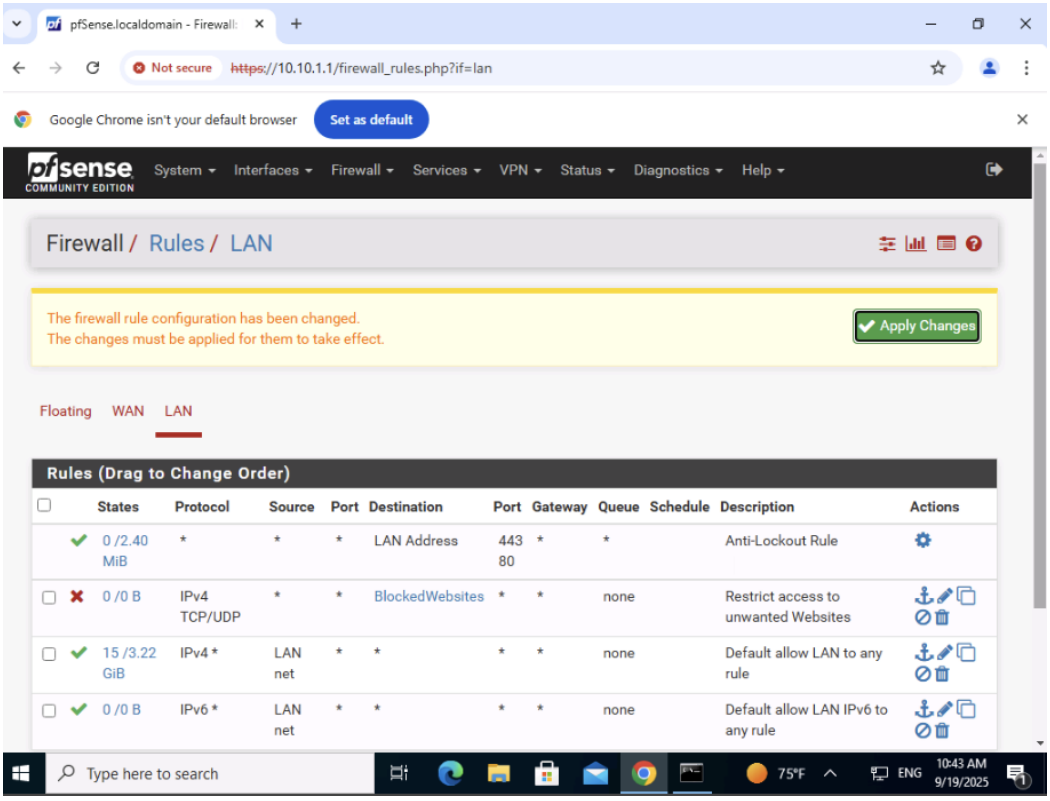

Admin Machine-1
pfSense.localdomain - Status: D
Not secure https://10.10.1.1
Google Chrome isn't your default browser
Set as default
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Status / Dashboard
System Information
Name pfSense.localdomain
User admin@10.10.1.2 (Local Database)
System Microsoft Azure
Netgate Device ID: 8db618da9856c98da024
BIOS Vendor: American Megatrends Inc.
Version: 090008
Release Date: Fri Dec 7 2018
Version 2.4.5-RELEASE-p1 (amd64)
built on Tue Jun 02 17:51:17 EDT 2020
FreeBSD 11.3-STABLE
The system is on the latest version.
CPU Type Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz
AES-NI CPU Crypto: Yes (inactive)
Kernel PTI Disabled
MDS Mitigation Inactive
Netgate Services And Support
Contract type Community Support
Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
Upgrade Your Support
Community Support Resources
Type here to search
Enzo...
ENG
10:25 AM
9/19/2025

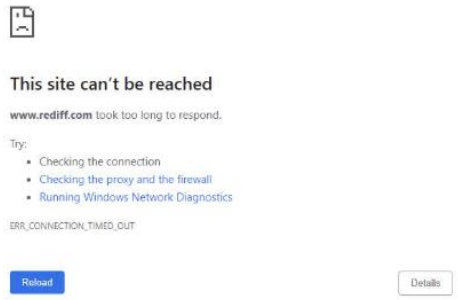

Admin Machine-1
pfSense.localdomain - Firewall:
Not secure
https://10.10.1.1/firewall_aliases_edit.php?tab=ip
Google Chrome isn't your default browser
Set as default
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Aliases / Edit
Properties
Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description
A description may be entered here for administrative reference (not parsed).
Type
Host(s)
Host(s)
Hint
Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.
IP or FQDN
Address
Description
Save
Add Host
Type here to search
Enzo...
ENG
10:25 AM
9/19/2025


Admin Machine-1
Command Prompt
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Admin>ping rediff.com
Pinging rediff.com [95.100.104.34] with 32 bytes of data:
Reply from 95.100.104.34: bytes=32 time=2ms TTL=55
Reply from 95.100.104.34: bytes=32 time=2ms TTL=55
Reply from 95.100.104.34: bytes=32 time=2ms TTL=55
Reply from 95.100.104.34: bytes=32 time=2ms TTL=55
Ping statistics for 95.100.104.34:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 2ms, Average = 2ms
C:\Users\Admin>


Admin Machine-1
pfSense.localdomain - Firewall:
Not secure
https://10.10.1.1/firewall_aliases_edit.php?tab=ip
Google Chrome isn't your default browser
Set as default
Firewall / Aliases / Edit
Properties
Name
BlockedWebsites
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description
Restrict the access of unwanted websites
A description may be entered here for administrative reference (not parsed).
Type
Host(s)
Host(s)
Hint
Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.
IP or FQDN
www.rediff.com
Site URL
Delete
84.53.185.208
Site IP Address
Delete
Save
Add Host
Type here to search
75°F
ENG
10:40 AM
9/19/2025


pfSense.localdomain - Firewall:
Not secure https://10.10.1.1/firewall_aliases.php?tab=ip
Google Chrome isn't your default browser
Set as default
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Firewall / Aliases / IP
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
IP Ports URLs All
Firewall Aliases IP
Name Values Description Actions
BlockedWebsites www.rediff.com, 84.53.185.208 Restrict the access of unwanted websites
Add Import
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.
Type here to search
75°F
ENG
10:40 AM
9/19/2025


pfSense.localdomain - Firewall:
Not secure https://10.10.1.1/firewall_rules.php?if=lan
Google Chrome isn't your default browser
Set as default
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Firewall / Rules / LAN
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
Floating WAN LAN
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
0 /2.40 MiB * * * LAN Address 443 80 * * Anti-Lockout Rule
0 /0 B IPv4 TCP/UDP * * BlockedWebsites * * none Restrict access to unwanted Websites
15 /3.22 GiB IPv4 * LAN net * * * * none Default allow LAN to any rule
0 /0 B IPv6 * LAN net * * * * none Default allow LAN IPv6 to any rule
Type here to search
75°F
ENG
10:43 AM
9/19/2025



Exercise 4: Implementing Network-Based Firewall Functionality: Blocking Insecure Ports using pfSense Firewall

The pfSense firewall/router helps network defenders in monitoring and controlling the inbound and outbound traffic of the network connections.

Lab Scenario

To keep the computer resources of the organization secure, network defenders need to configure outbound traffic because outbound traffic leaves the network vulnerable to malware that targets organizational resources. These threats can be protected by using firewall rules. The pfSense firewall allows specific traffic on specific ports while blocking all other traffic.

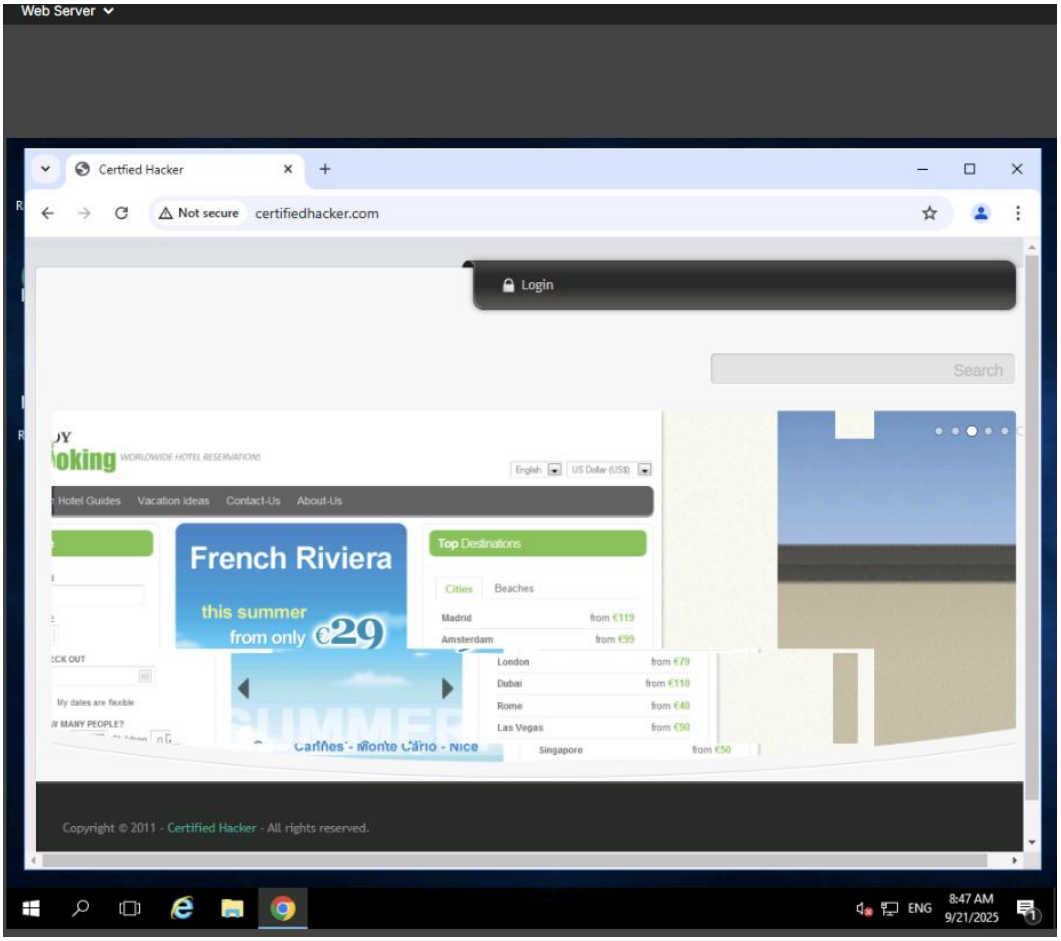
Lab Objectives

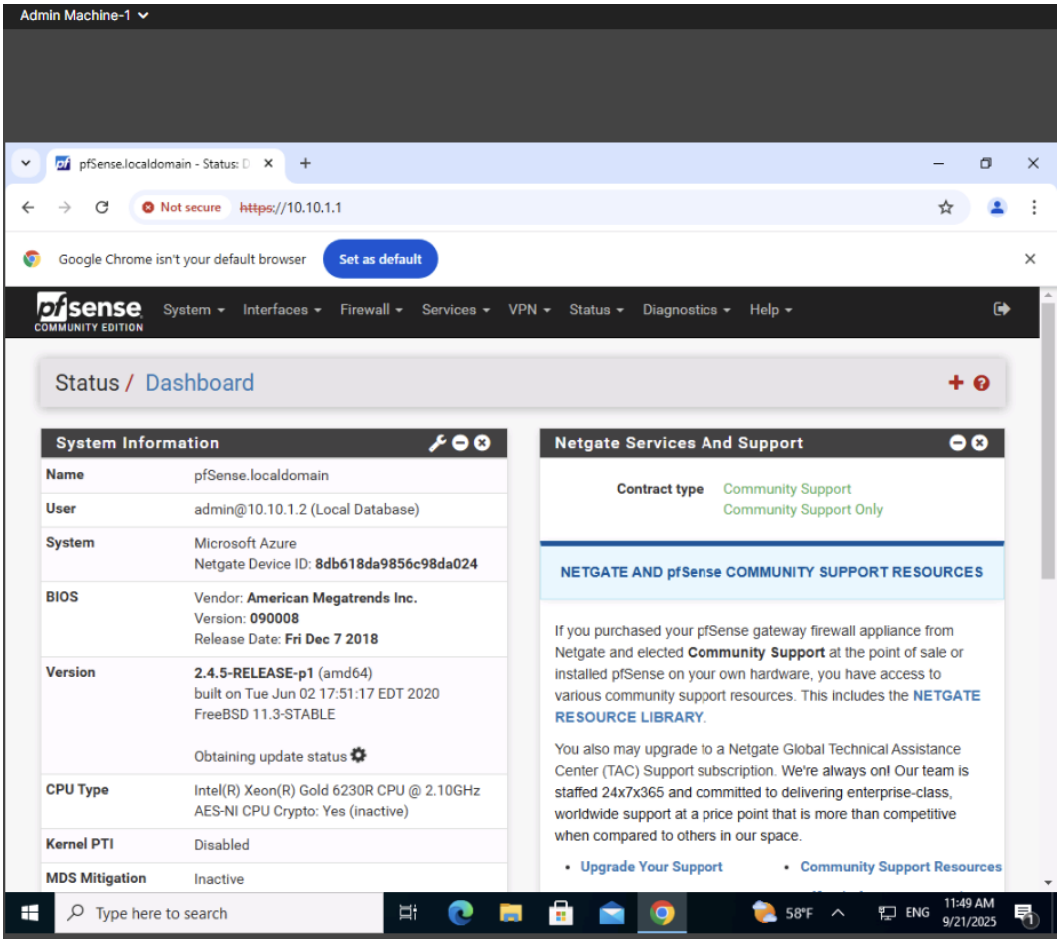
This lab will demonstrate how to block insecure ports using the pfSense firewall and protect endpoints within the network using the pfSense firewall.

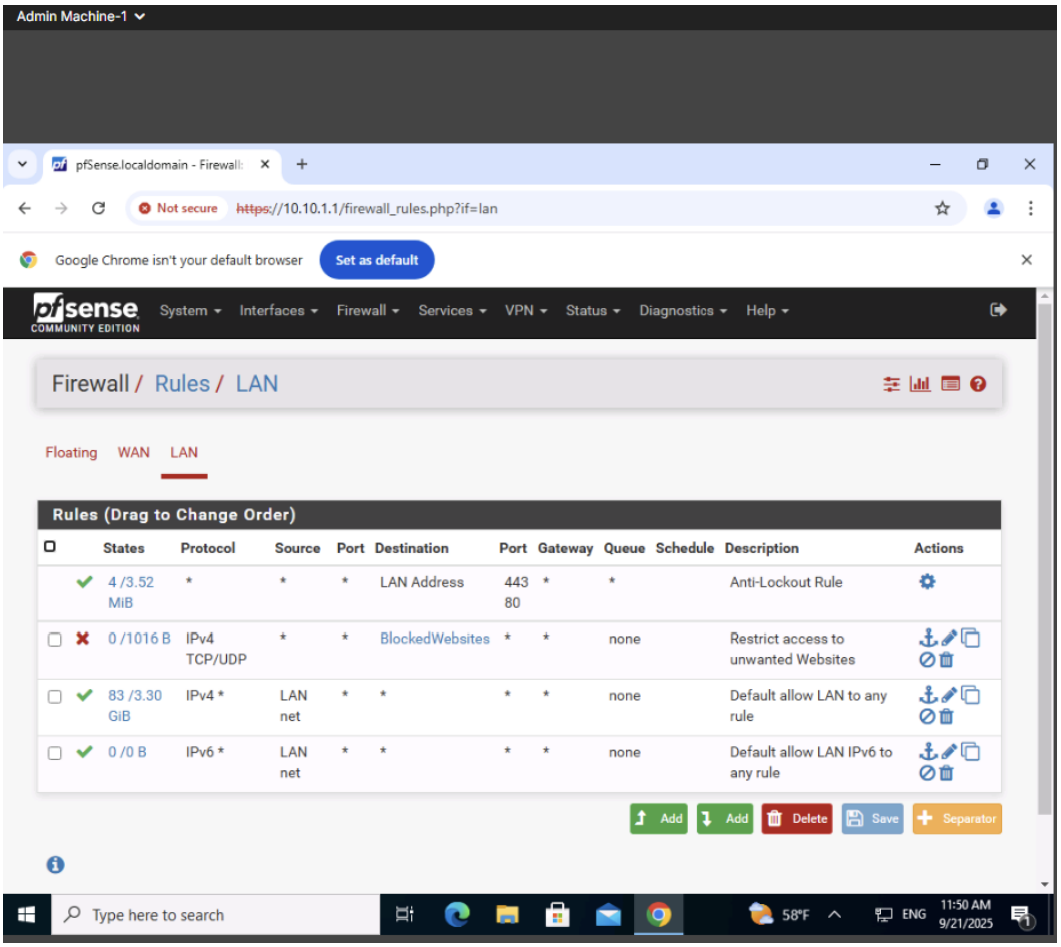
Overview of Firewall Rules

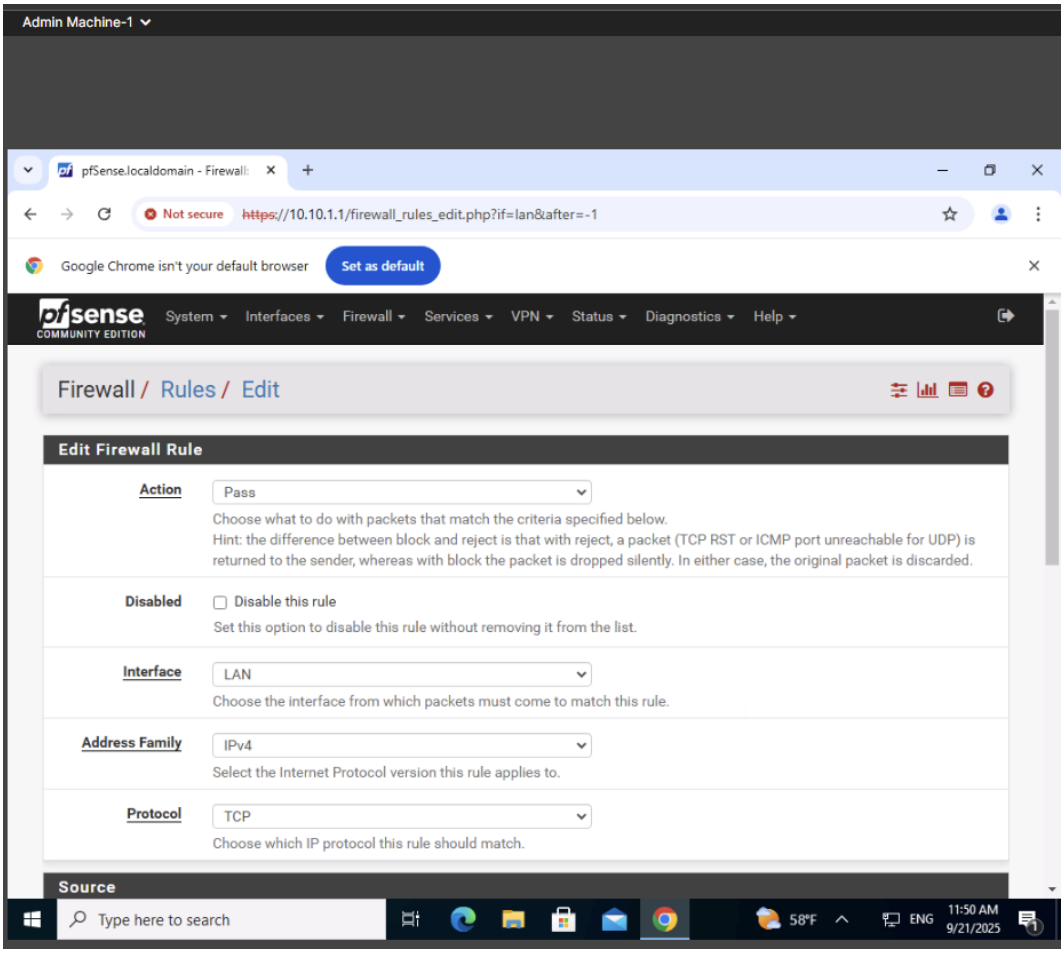
Firewall rules can be created for either inbound or outbound traffic.

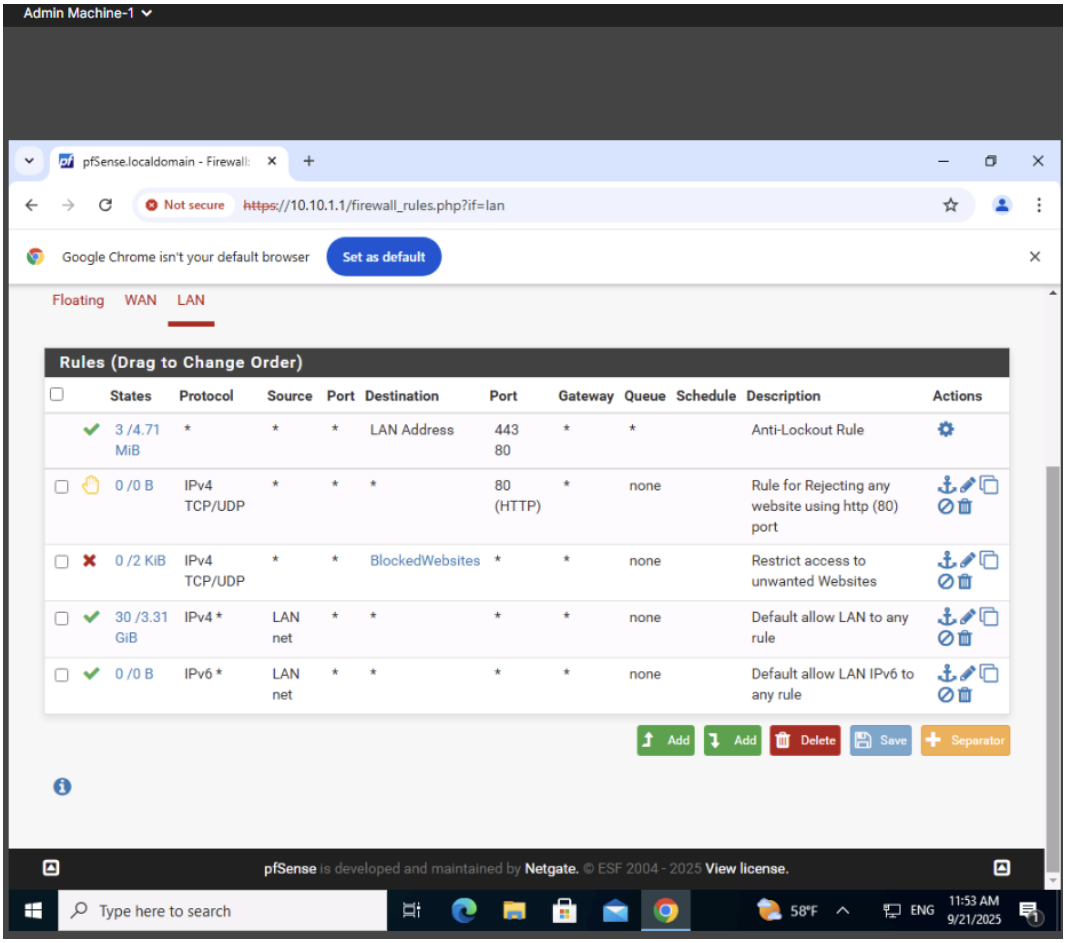
- An inbound firewall rule protects the network against incoming malicious traffic from the Internet or other network segments.
- An outbound firewall protects against outgoing traffic originating inside an enterprise network. Firewall rules can be configured to specify computers, users, programs, services, ports, and protocols.


Web Server
Certfied Hacker
Not secure
certifiedhacker.com
Login
Search
WORLDWIDE HOTEL RESERVATIONS
English
US Dollar (US$)
Hotel Guides
Vacation Ideas
Contact-Us
About-Us
French Riviera
this summer
from only €29
Top Destinations
Cities
Beaches
Madrid from €119
Amsterdam from €99
London from €79
Dubai from €110
Rome from €40
Las Vegas from €90
Singapore from €50
Cannes - Monte Carlo - Nice
Copyright © 2011 - Certified Hacker - All rights reserved.
ENG
8:47 AM
9/21/2025

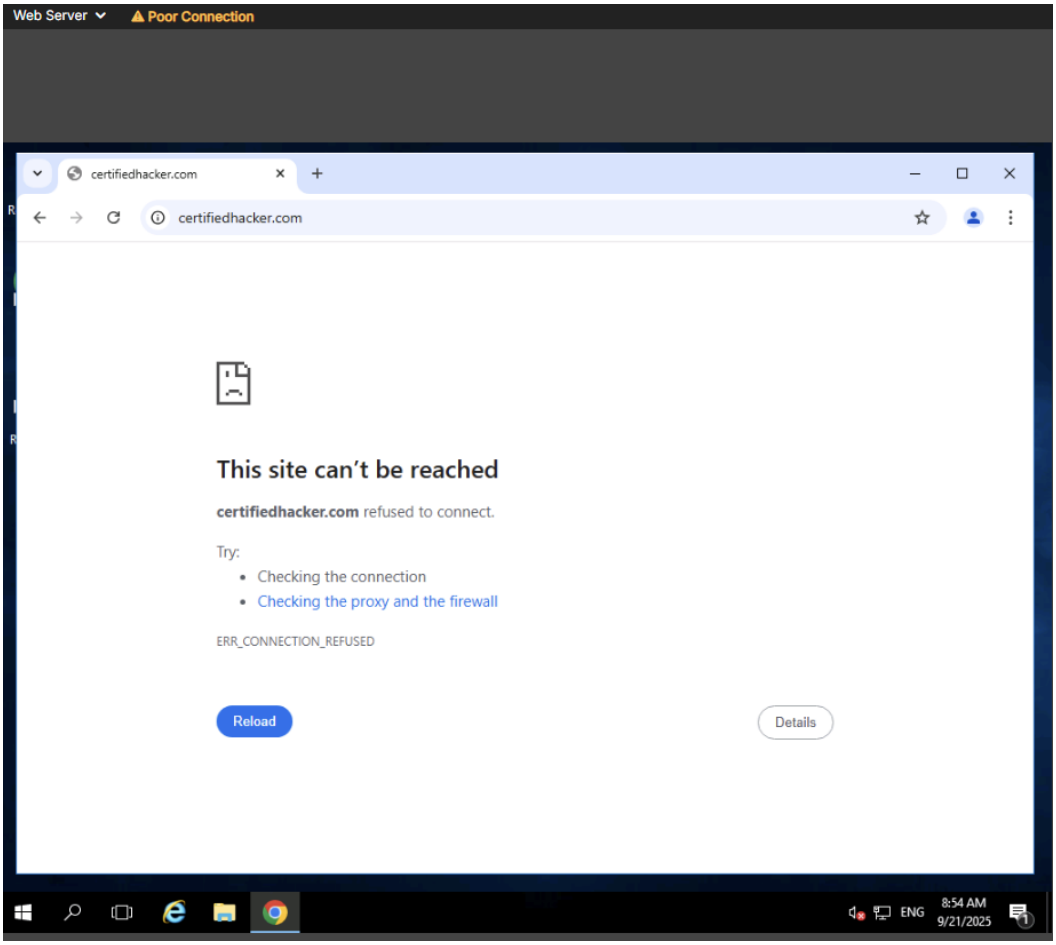

Admin Machine-1
pfSense.localdomain - Status: D
Not secure
https://10.10.1.1
Google Chrome isn't your default browser
Set as default
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / Dashboard
System Information
Name
pfSense.localdomain
User
admin@10.10.1.2 (Local Database)
System
Microsoft Azure
Netgate Device ID: 8db618da9856c98da024
BIOS
Vendor: American Megatrends Inc.
Version: 090008
Release Date: Fri Dec 7 2018
Version
2.4.5-RELEASE-p1 (amd64)
built on Tue Jun 02 17:51:17 EDT 2020
FreeBSD 11.3-STABLE
Obtaining update status
CPU Type
Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz
AES-NI CPU Crypto: Yes (inactive)
Kernel PTI
Disabled
MDS Mitigation
Inactive
Netgate Services And Support
Contract type
Community Support
Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
Upgrade Your Support
Community Support Resources
Type here to search
58°F
ENG
11:49 AM
9/21/2025

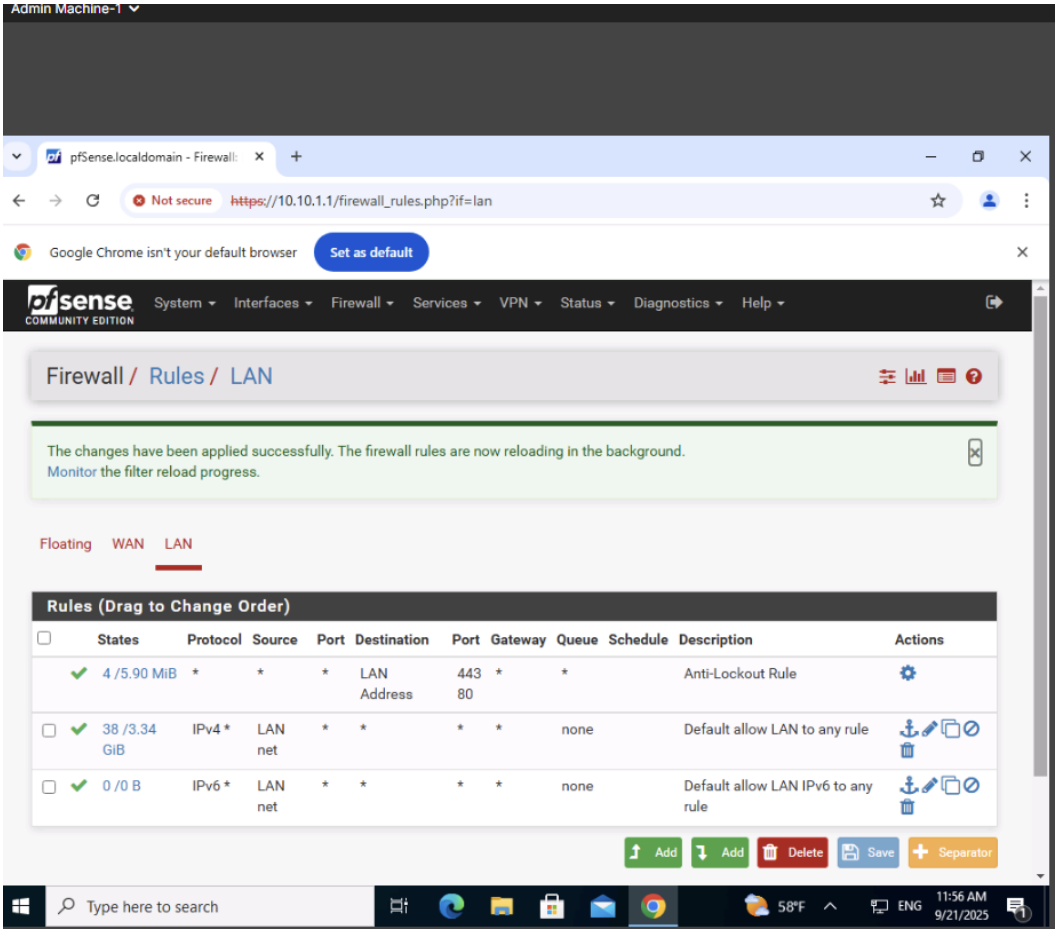

Admin Machine-1
pfSense.localdomain - Firewall:
Not secure
https://10.10.1.1/firewall_rules.php?if=lan
Google Chrome isn't your default browser
Set as default
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / LAN
Floating
WAN
LAN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
4 /3.52 MiB
*
*
*
LAN Address
443 80
*
*
Anti-Lockout Rule
0 /1016 B
IPv4 TCP/UDP
*
*
BlockedWebsites
*
*
none
Restrict access to unwanted Websites
83 /3.30 GiB
IPv4 *
LAN net
*
*
*
*
none
Default allow LAN to any rule
0 /0 B
IPv6 *
LAN net
*
*
*
*
none
Default allow LAN IPv6 to any rule
Add
Add
Delete
Save
Separator
Type here to search
58°F
ENG
11:50 AM
9/21/2025

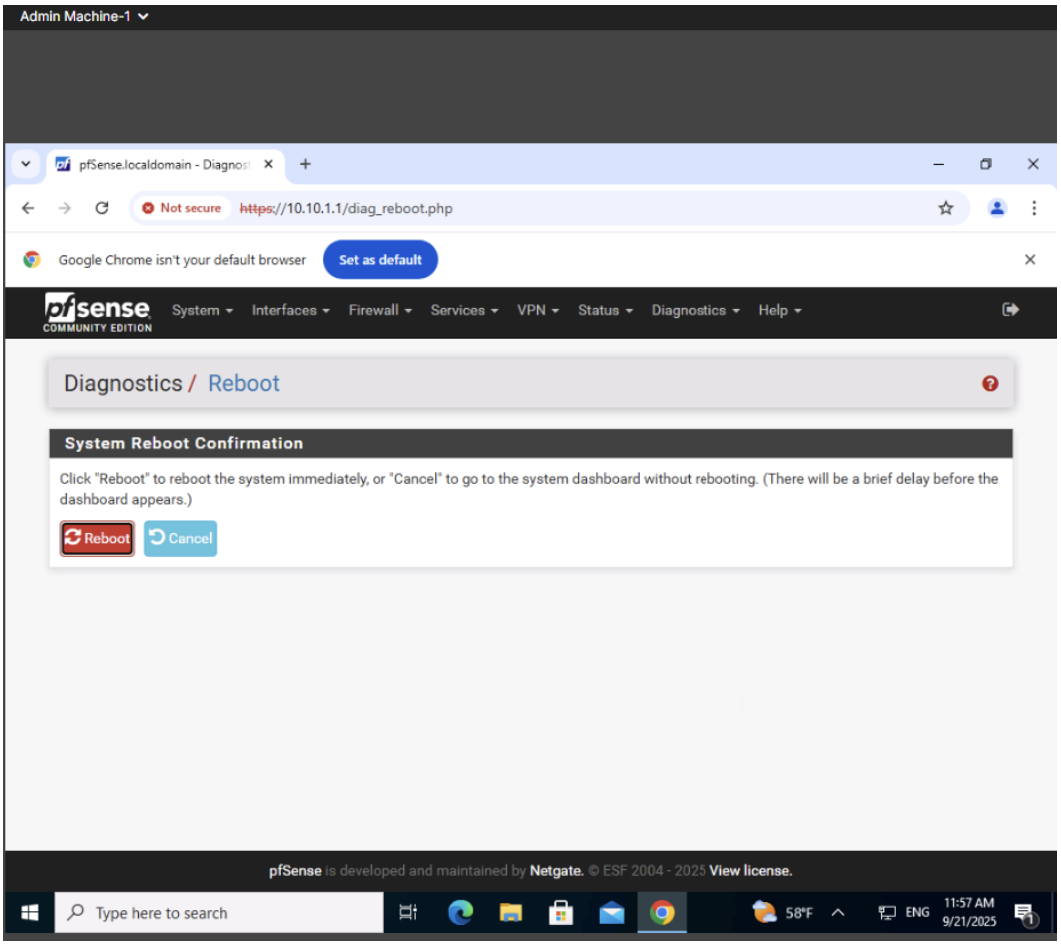

Admin Machine-1
pfSense.localdomain - Firewall:
Not secure
https://10.10.1.1/firewall_rules_edit.php?if=lan&after=-1
Google Chrome isn't your default browser
Set as default
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / Edit
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
LAN
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP
Choose which IP protocol this rule should match.
Source
Type here to search
58°F
ENG
11:50 AM
9/21/2025

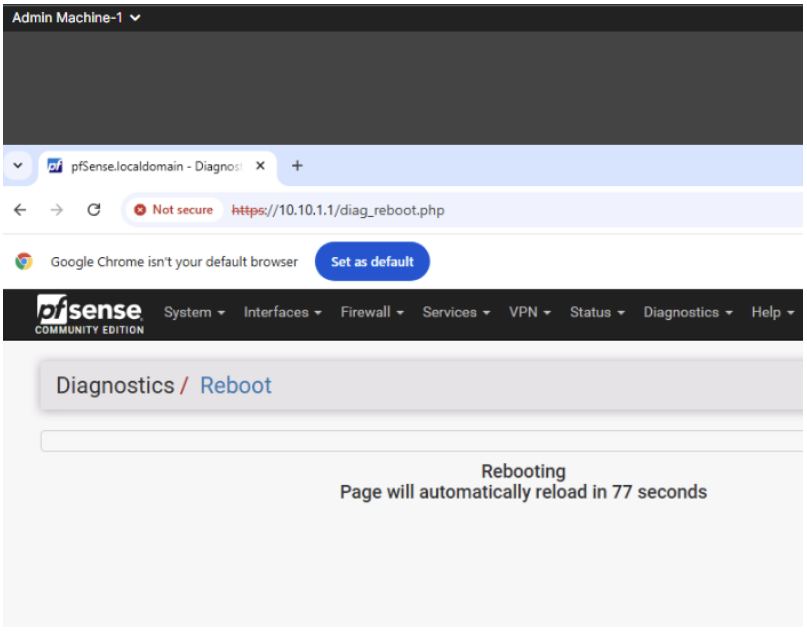


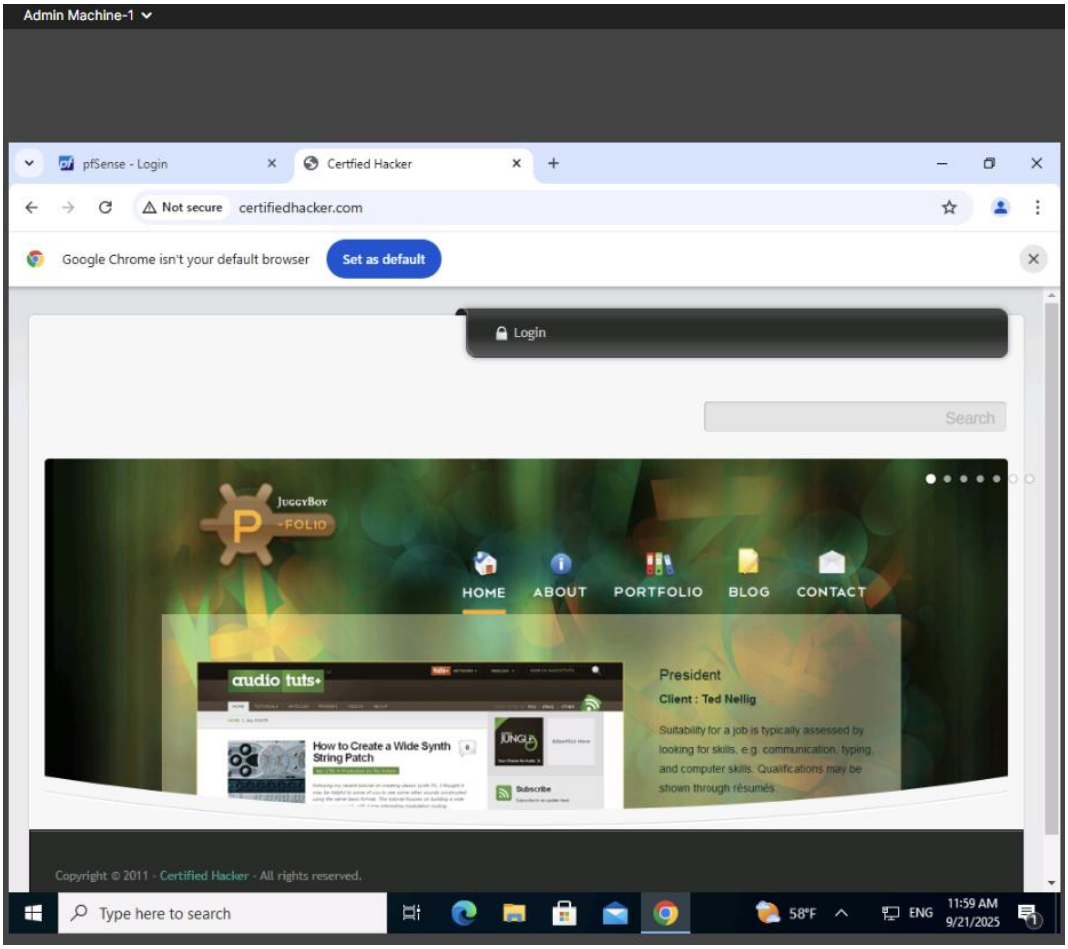
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

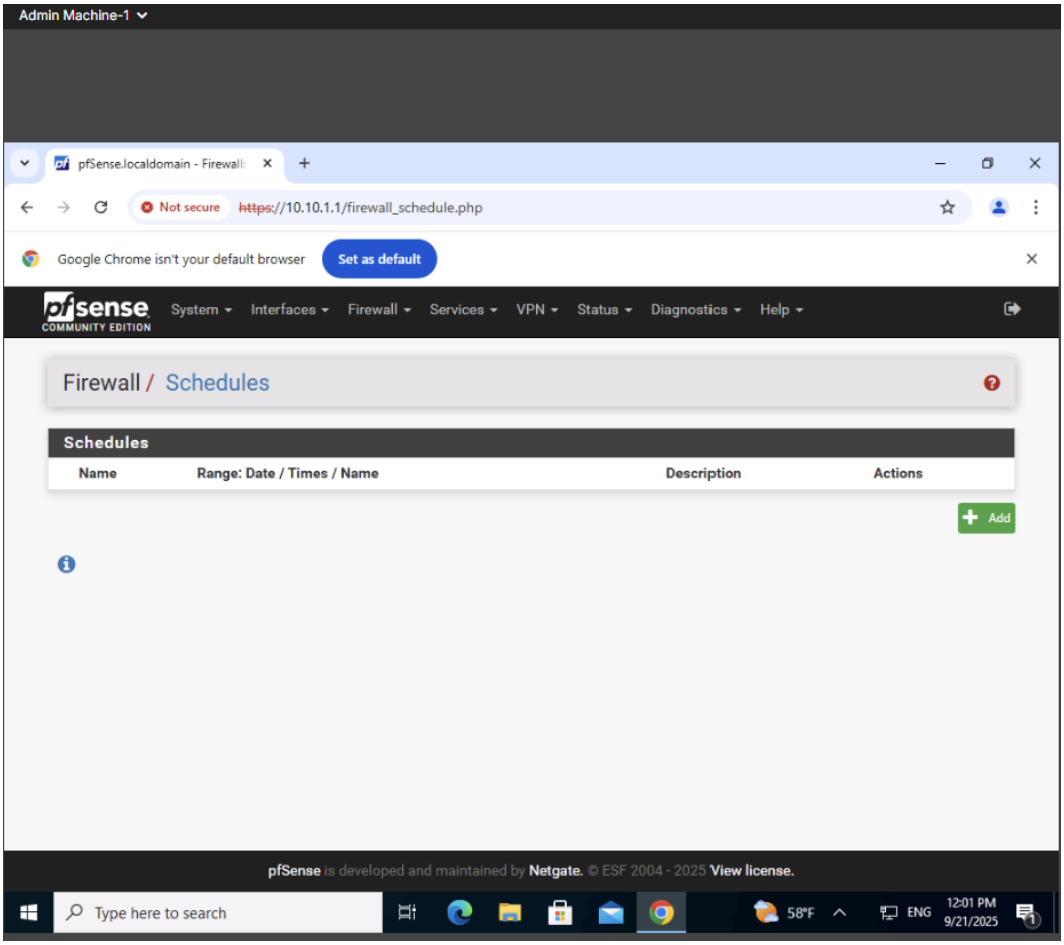

Web Server
Poor Connection
certifiedhacker.com
certifiedhacker.com
This site can't be reached
certifiedhacker.com refused to connect.
Try:
Checking the connection
Checking the proxy and the firewall
ERR_CONNECTION_REFUSED
Reload
Details
ENG
8:54 AM
9/21/2025

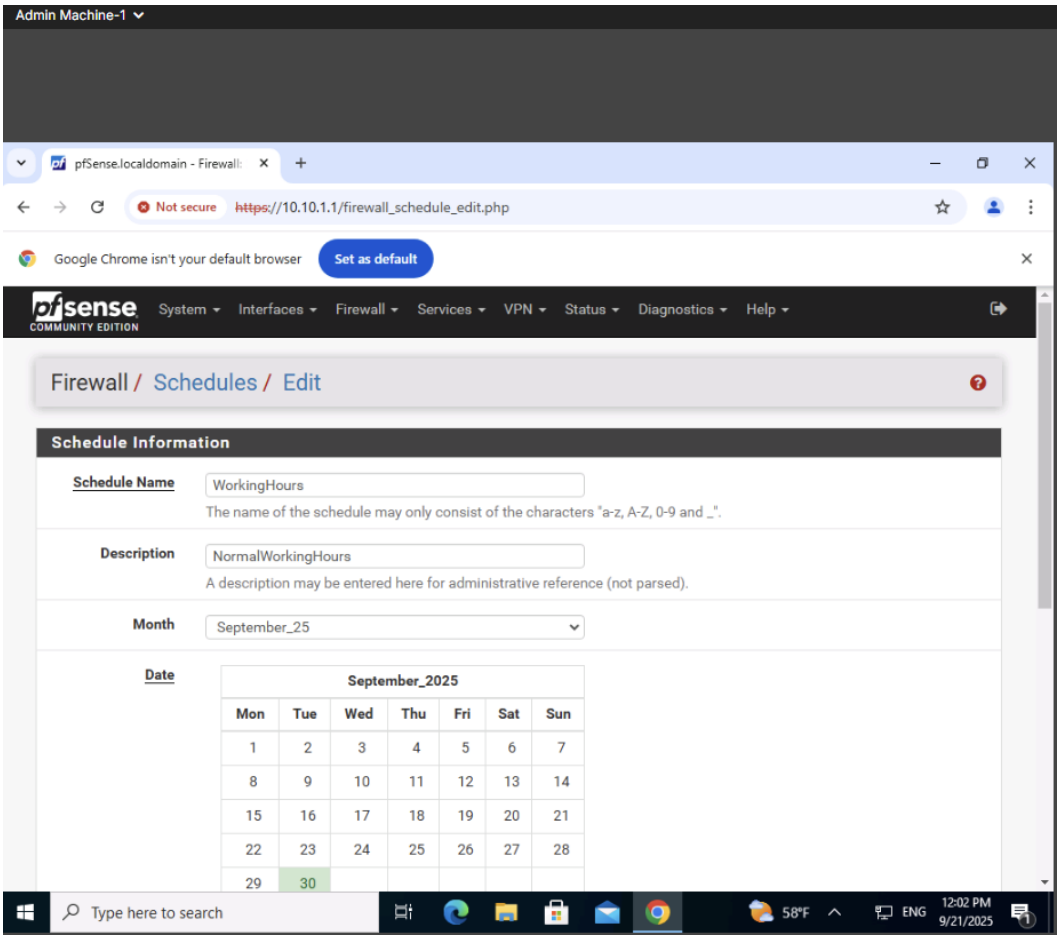

Admin Machine-1
pfSense.localdomain - Firewall:
Not secure
https://10.10.1.1/firewall_rules.php?if=lan
Google Chrome isn't your default browser
Set as default
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / LAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating
WAN
LAN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
4 /5.90 MiB * * * LAN Address 443 80 * * Anti-Lockout Rule
38 /3.34 GiB IPv4 * LAN net * * * * none Default allow LAN to any rule
0 /0 B IPv6 * LAN net * * * * none Default allow LAN IPv6 to any rule
Add
Add
Delete
Save
Separator
Type here to search
58°F
ENG
11:56 AM
9/21/2025

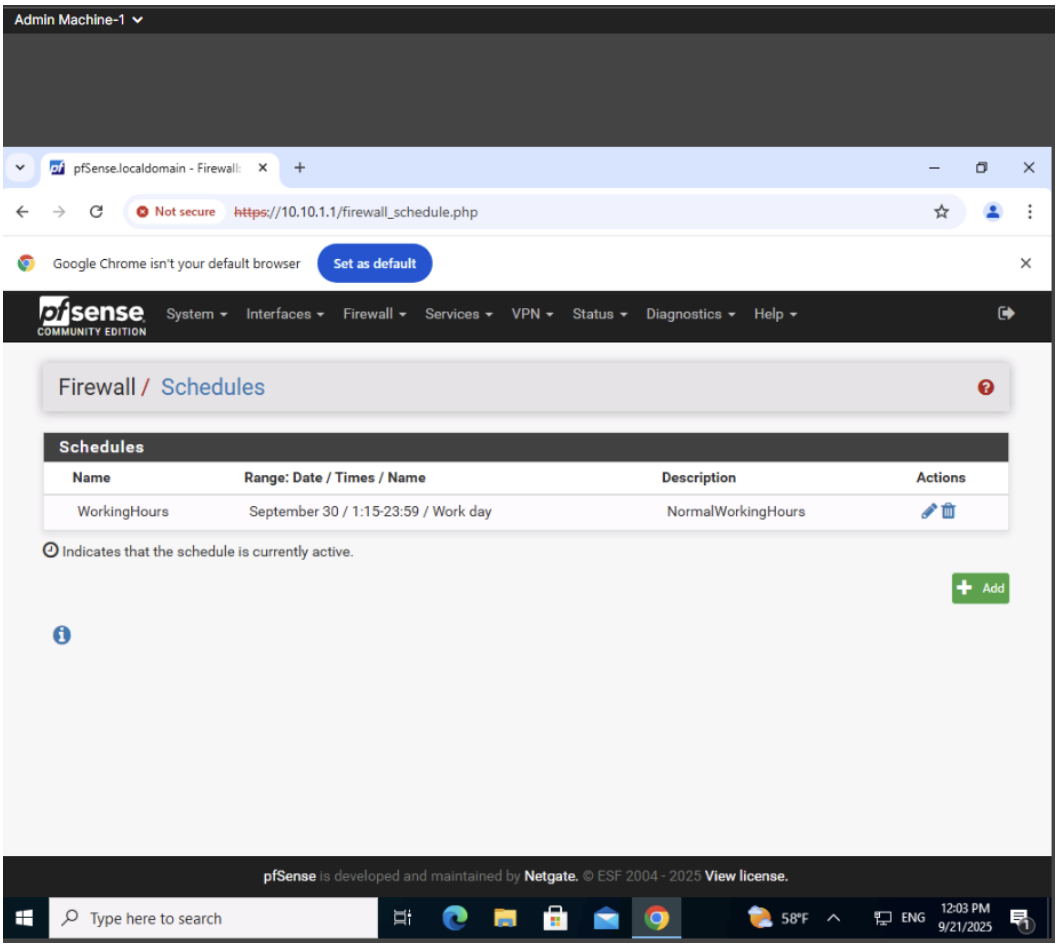

Admin Machine-1
pfSense.localdomain - Diagnos
Not secure https://10.10.1.1/diag_reboot.php
Google Chrome isn't your default browser
Set as default
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Diagnostics / Reboot
System Reboot Confirmation
Click "Reboot" to reboot the system immediately, or "Cancel" to go to the system dashboard without rebooting. (There will be a brief delay before the dashboard appears.)
Reboot
Cancel
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.
Type here to search
58°F
ENG
11:57 AM
9/21/2025

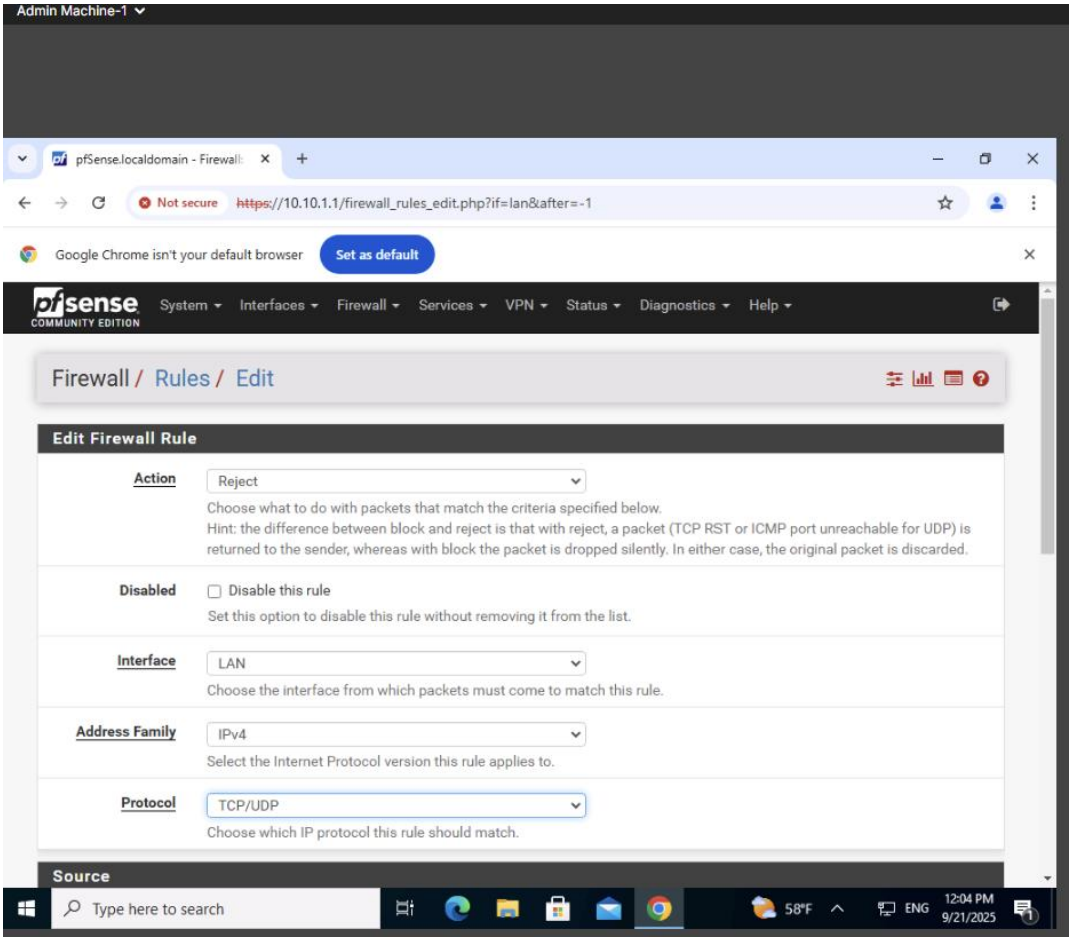

Admin Machine-1
pfSense.localdomain - Diagnos
Not secure https://10.10.1.1/diag_reboot.php
Google Chrome isn't your default browser
Set as default
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Diagnostics / Reboot
Rebooting
Page will automatically reload in 77 seconds

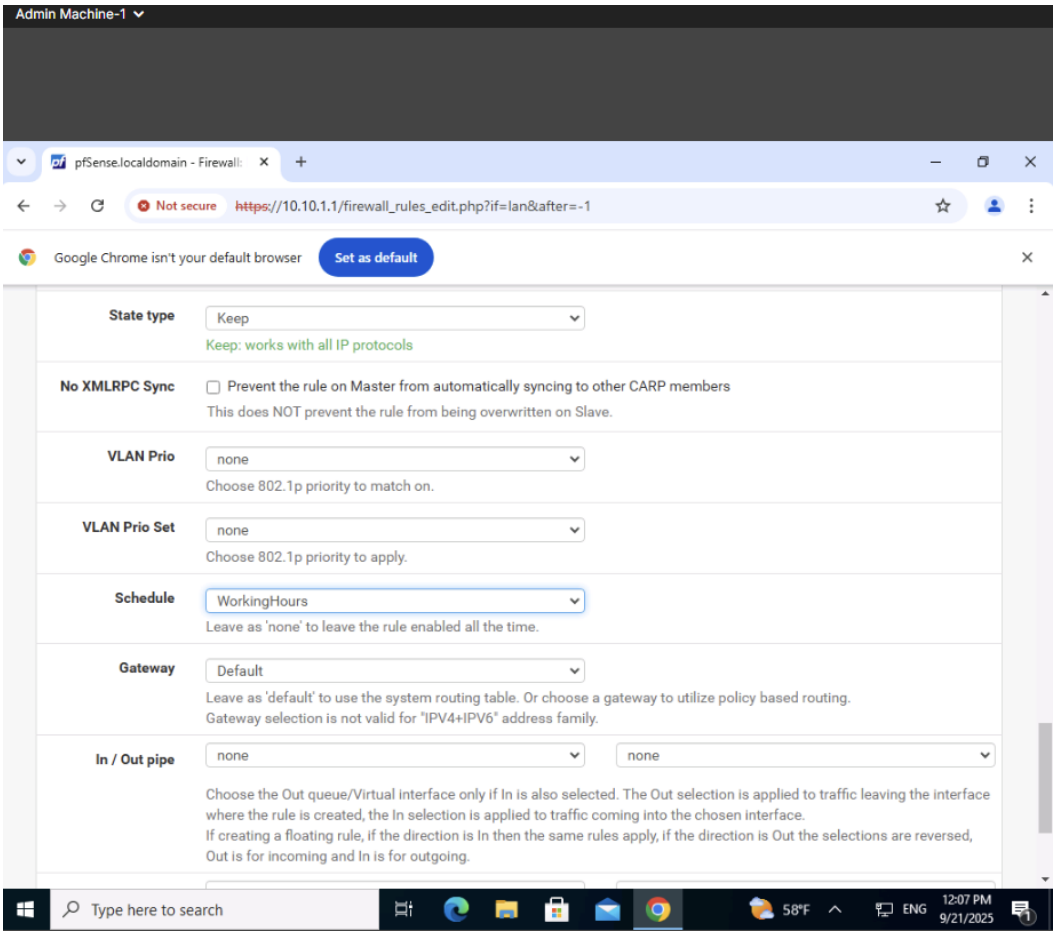

Admin Machine-1
pfSense - Login
Certfied Hacker
Not secure
certifiedhacker.com
Google Chrome isn't your default browser
Set as default
Login
Search
JuggyBoy
P -FOLIO
HOME
ABOUT
PORTFOLIO
BLOG
CONTACT
audio tuts+
How to Create a Wide Synth String Patch
Subscribe
President
Client : Ted Nellig
Suitability for a job is typically assessed by looking for skills, e.g. communication, typing, and computer skills. Qualifications may be shown through résumés.
Copyright © 2011 - Certified Hacker - All rights reserved.
Type here to search
58°F
ENG
11:59 AM
9/21/2025

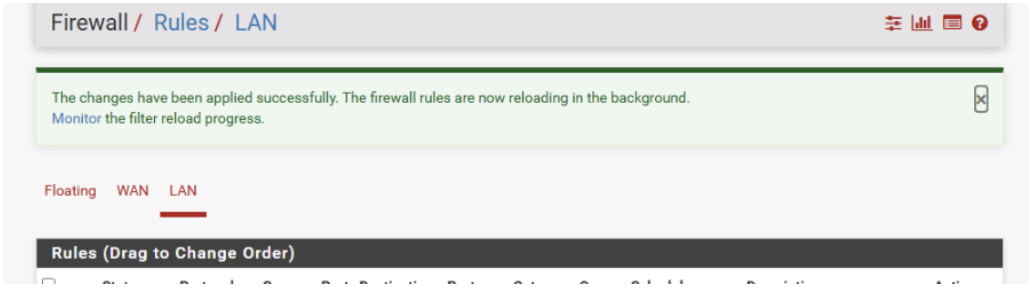

Admin Machine-1
pfSense.localdomain - Firewall:
Not secure
https://10.10.1.1/firewall_schedule.php
Google Chrome isn't your default browser
Set as default
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Schedules
Schedules
Name
Range: Date / Times / Name
Description
Actions
Add
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.
Type here to search
58°F
ENG
12:01 PM
9/21/2025

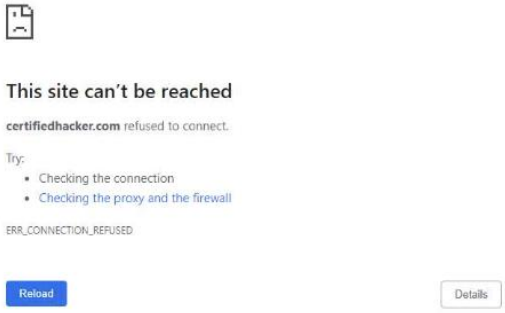

Admin Machine-1
pfSense.localdomain - Firewall:
Not secure
https://10.10.1.1/firewall_schedule_edit.php
Google Chrome isn't your default browser
Set as default
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Schedules / Edit
Schedule Information
Schedule Name
WorkingHours
The name of the schedule may only consist of the characters "a-z, A-Z, 0-9 and _".
Description
NormalWorkingHours
A description may be entered here for administrative reference (not parsed).
Month
September_25
Date
September_2025
Mon Tue Wed Thu Fri Sat Sun
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Type here to search
58°F
ENG
12:02 PM
9/21/2025


Admin Machine-1
pfSense.localdomain - Firewall:
Not secure
https://10.10.1.1/firewall_schedule.php
Google Chrome isn't your default browser
Set as default
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Schedules
Schedules
Name
Range: Date / Times / Name
Description
Actions
WorkingHours
September 30 / 1:15-23:59 / Work day
NormalWorkingHours
Indicates that the schedule is currently active.
Add
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.
Type here to search
58°F
ENG
12:03 PM
9/21/2025


Admin Machine-1
pfSense.localdomain - Firewall
Not secure
https://10.10.1.1/firewall_rules_edit.php?if=lan&after=-1
Google Chrome isn't your default browser
Set as default
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / Edit
Edit Firewall Rule
Action
Reject
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
LAN
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP/UDP
Choose which IP protocol this rule should match.
Source
Type here to search
58°F
ENG
12:04 PM
9/21/2025


Admin Machine-1
pfSense.localdomain - Firewall:
Not secure
https://10.10.1.1/firewall_rules_edit.php?if=lan&after=-1
Google Chrome isn't your default browser
Set as default
State type
Keep
Keep: works with all IP protocols
No XMLRPC Sync
Prevent the rule on Master from automatically syncing to other CARP members
This does NOT prevent the rule from being overwritten on Slave.
VLAN Prio
none
Choose 802.1p priority to match on.
VLAN Prio Set
none
Choose 802.1p priority to apply.
Schedule
WorkingHours
Leave as 'none' to leave the rule enabled all the time.
Gateway
Default
Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.
Gateway selection is not valid for "IPV4+IPV6" address family.
In / Out pipe
none
none
Choose the Out queue/Virtual interface only if In is also selected. The Out selection is applied to traffic leaving the interface where the rule is created, the In selection is applied to traffic coming into the chosen interface.
If creating a floating rule, if the direction is In then the same rules apply, if the direction is Out the selections are reversed, Out is for incoming and In is for outgoing.
Type here to search
58°F
ENG
12:07 PM
9/21/2025


Firewall / Rules / LAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating
WAN
LAN
Rules (Drag to Change Order)


This site can't be reached
certifiedhacker.com refused to connect.
Try:
Checking the connection
Checking the proxy and the firewall
ERR_CONNECTION_REFUSED
Reload
Details

Exercise 5: Implementing Host-Based IDS Functionality using Wazuh HIDS

Host Intrusion Detection is a requirement for today's networks. Host-based Intrusion Detection Systems (HIDS) detect the events on the server and generate alerts. Attacks and threats can be monitored easily because the full communication stream can be inspected using HIDS.

Lab Scenario

Intrusion Detection Systems (IDS) help monitor network activity. HIDS enables a network defender to monitor the network traffic for malicious activity or policy violations. Using Wazuh enables network defenders to perform continuous monitoring and respond to advanced threats.

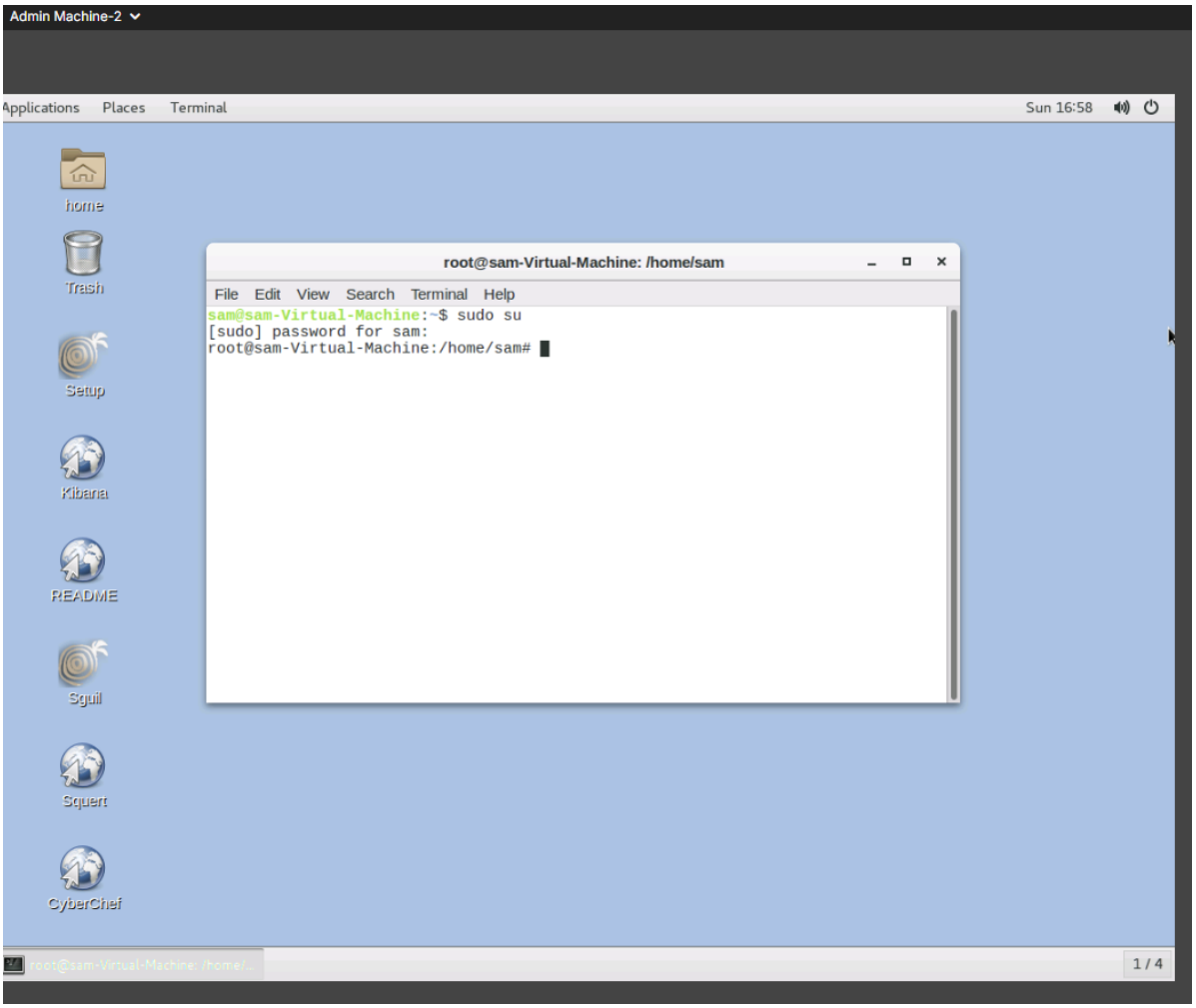
Lab Objectives

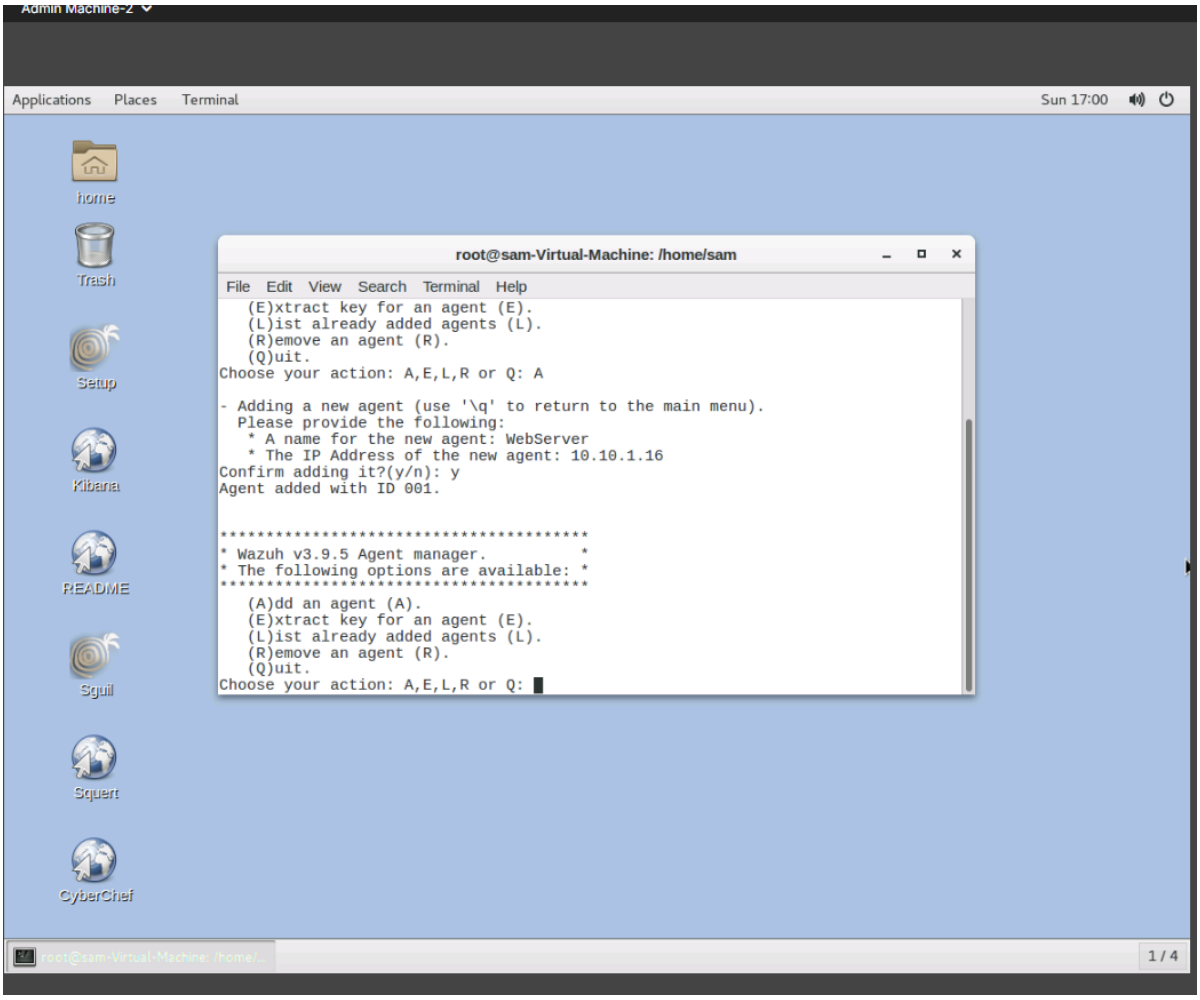
This lab will demonstrate the use of Wazuh HIDS and agent to capture network traffic and show how to monitor the captured traffic for malicious activities. In this lab, you will learn:

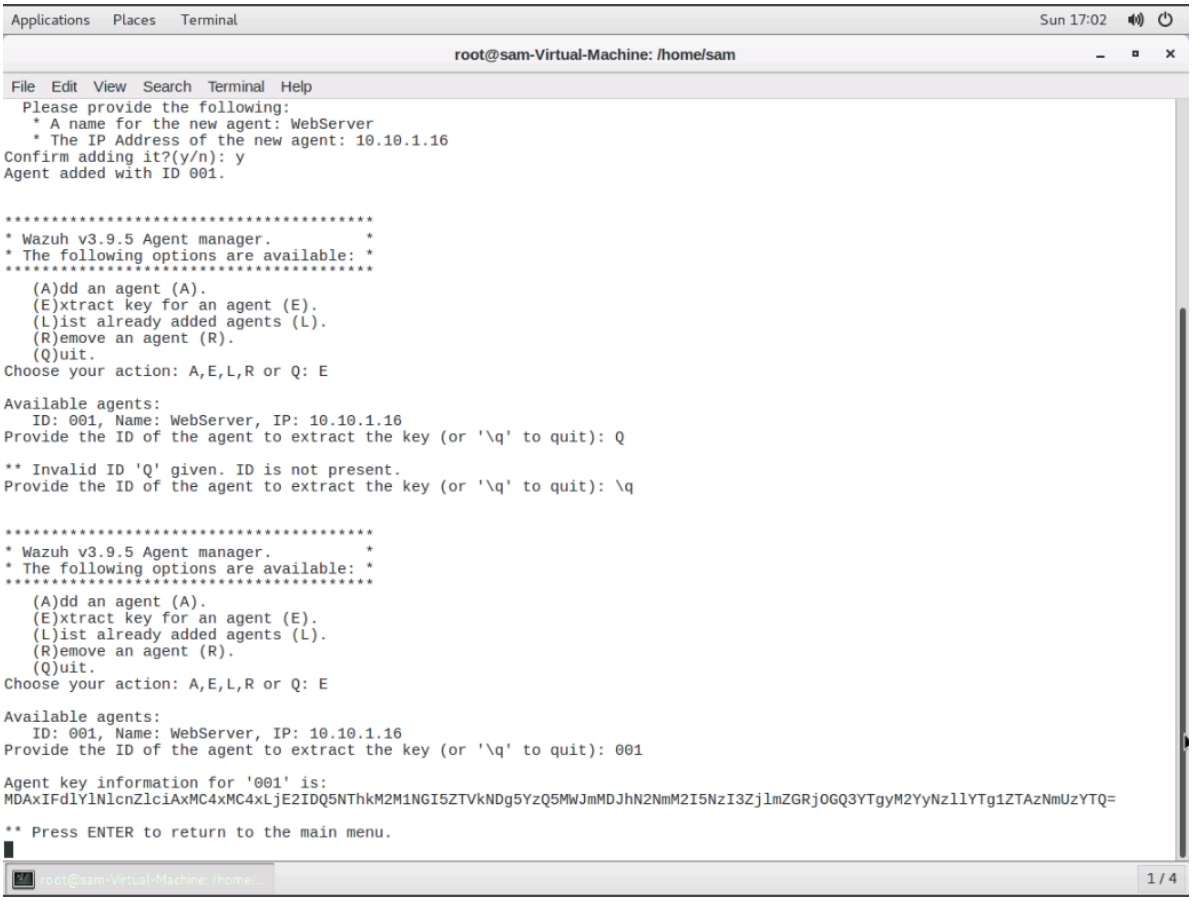
- Installing and configuring Wazuh HIDS and Wazuh agent
- Monitoring network traffic for malicious activity using Sguil

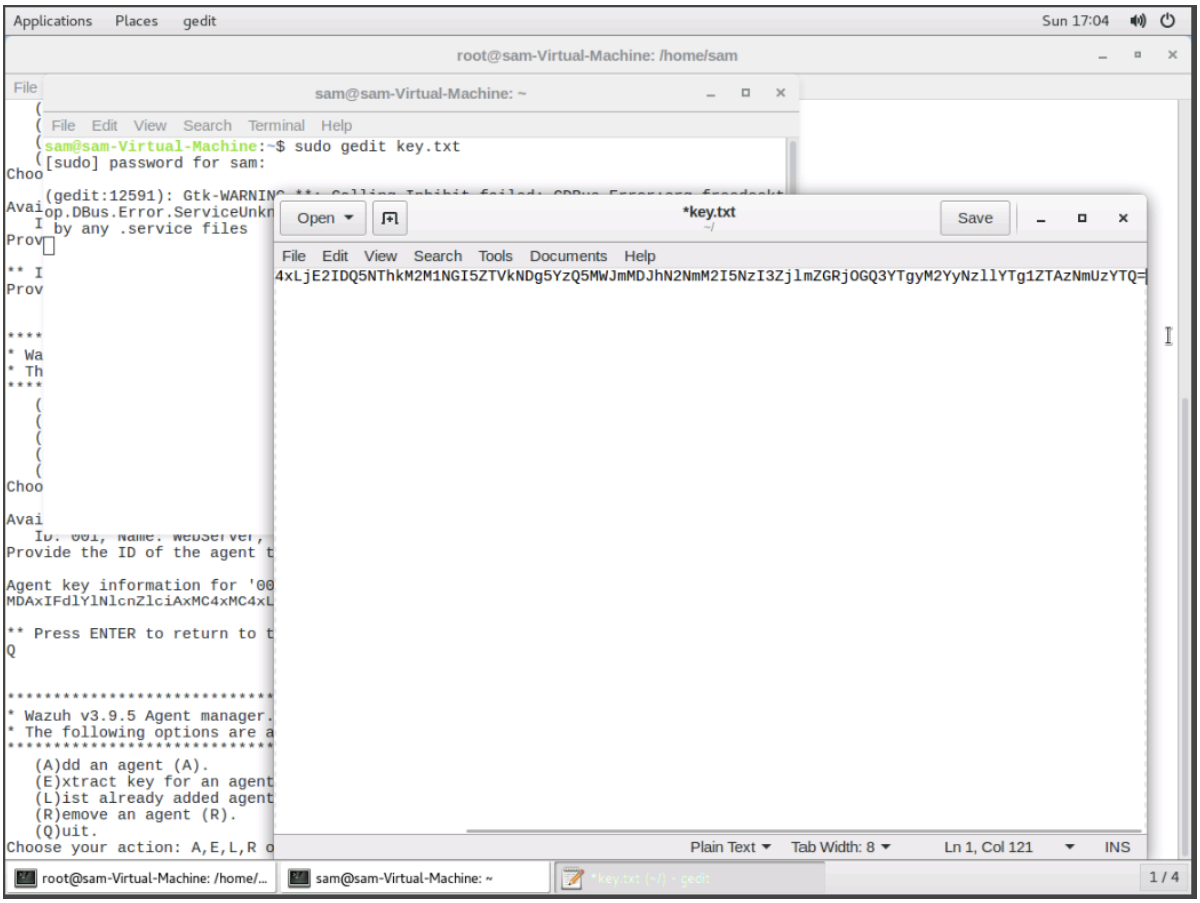
Overview of the Lab

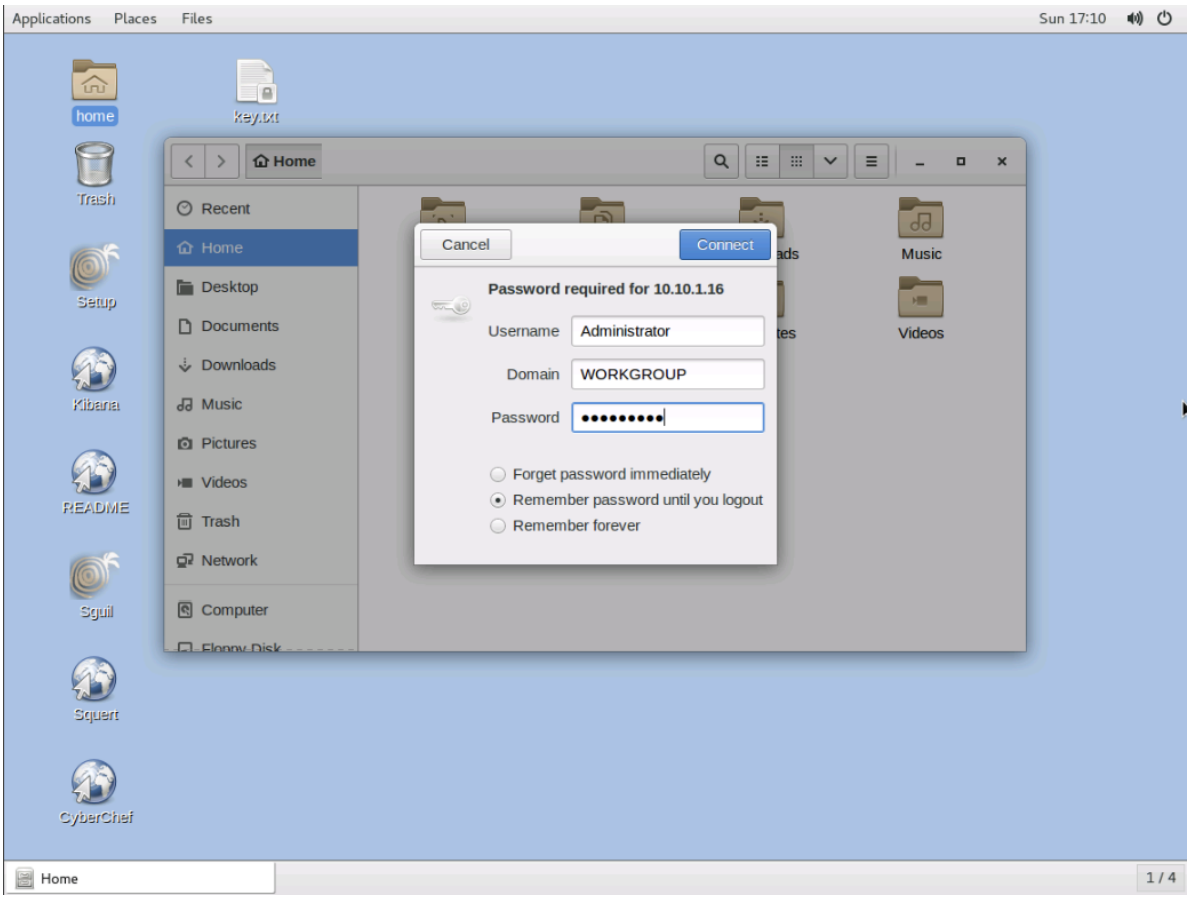
Wazuh (OSSEC) is an open-source HIDS. The Wazuh agent runs at a host-level, combining anomaly and signature-based technologies to detect intrusions or software misuse. It can also be used to monitor user activities, assess system configuration, and detect vulnerabilities. Sguil is an open-source interface for network security monitoring and event-driven analysis of IDS alerts (Snort and Barnyard). It consists of an intuitive GUI for accessing real-time events, session data, and network traffic capture.

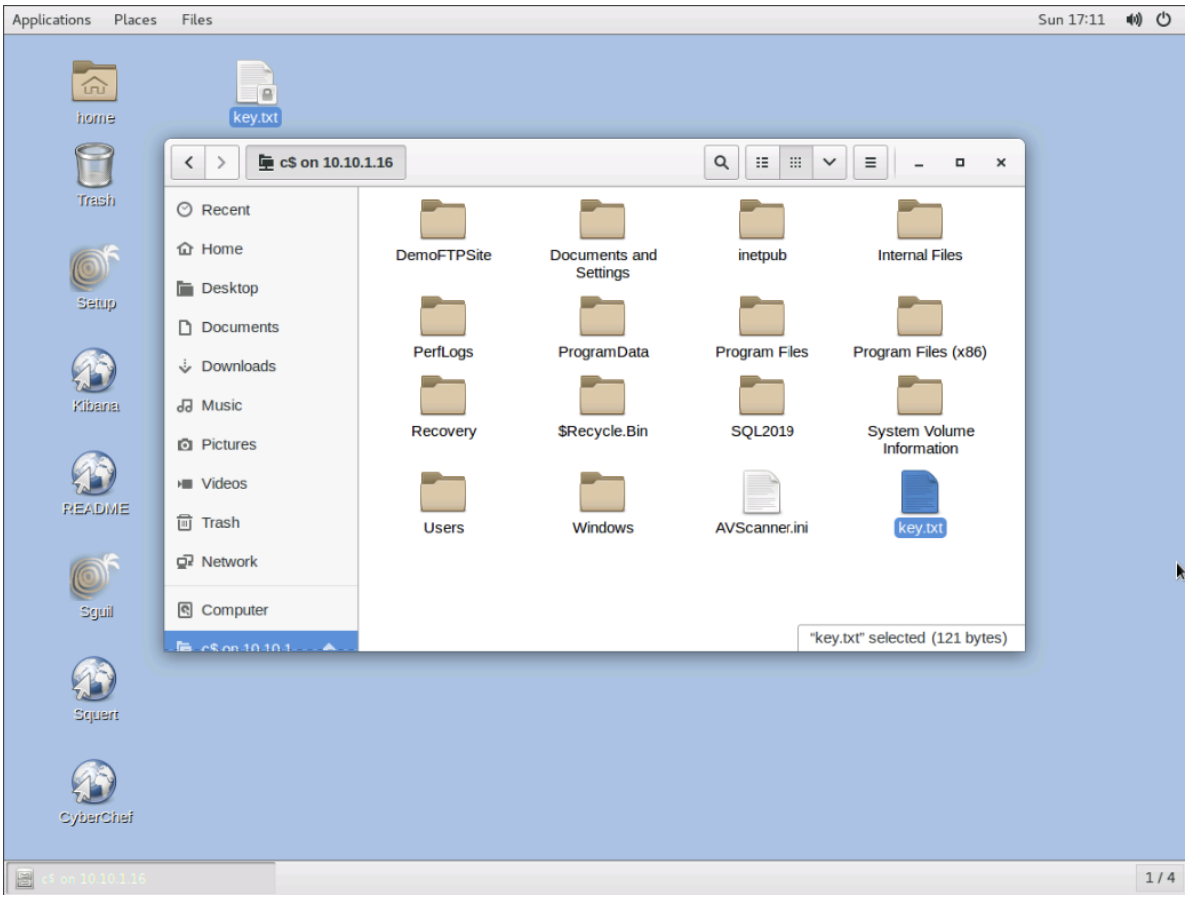

Admin Machine-2
Applications
Places
Terminal
Sun 16:58
home
Trash
Setup
Kibana
README
Sguil
Squert
CyberChef
root@sam-Virtual-Machine: /home/sam
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ sudo su
[sudo] password for sam:
root@sam-Virtual-Machine:/home/sam#
1 / 4

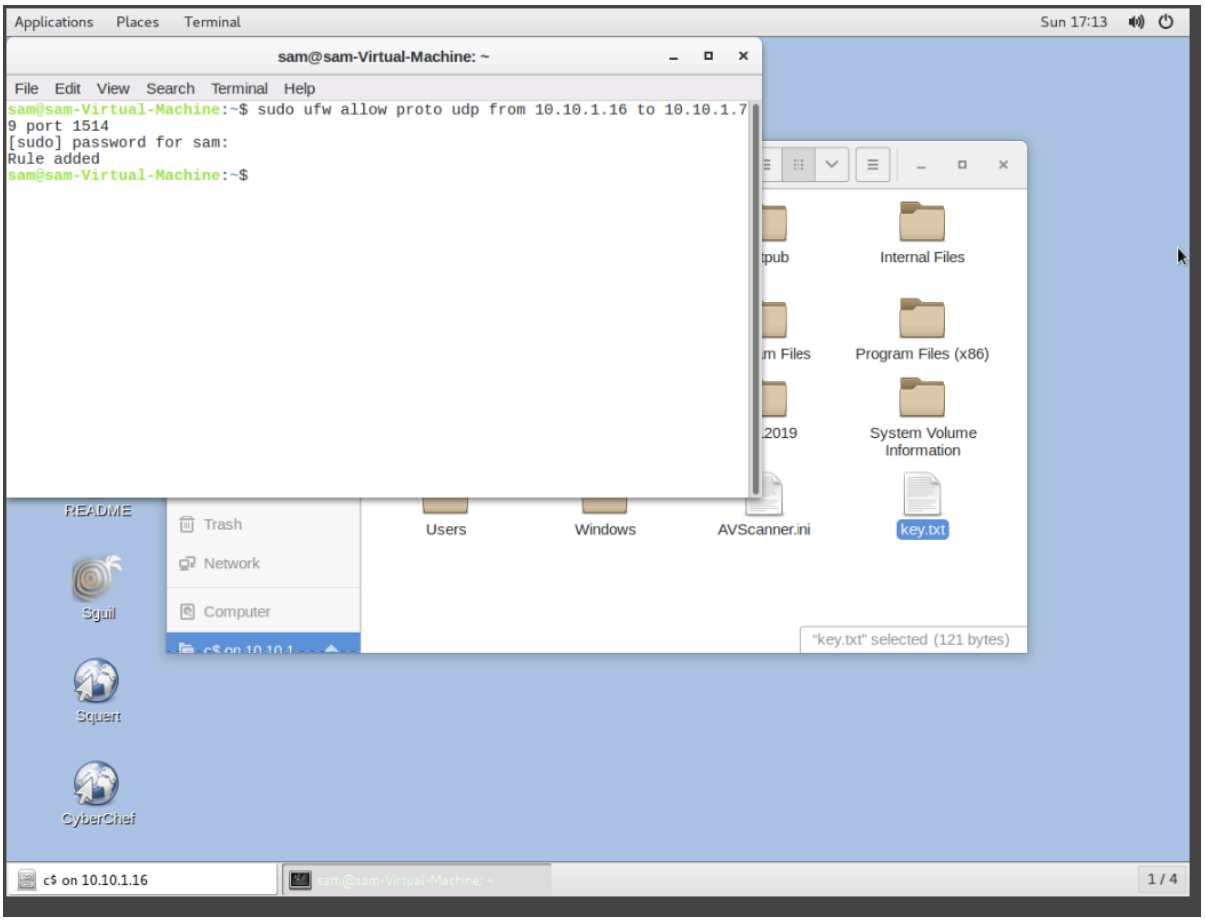

Admin Machine-2
Applications
Places
Terminal
Sun 17:00
home
Trash
Setup
Kibana
README
Sguil
Squert
CyberChef
root@sam-Virtual-Machine: /home/sam
File Edit View Search Terminal Help
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: A
- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: WebServer
* The IP Address of the new agent: 10.10.1.16
Confirm adding it?(y/n): y
Agent added with ID 001.
****
* Wazuh v3.9.5 Agent manager. *
* The following options are available: *
****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q:
1 / 4

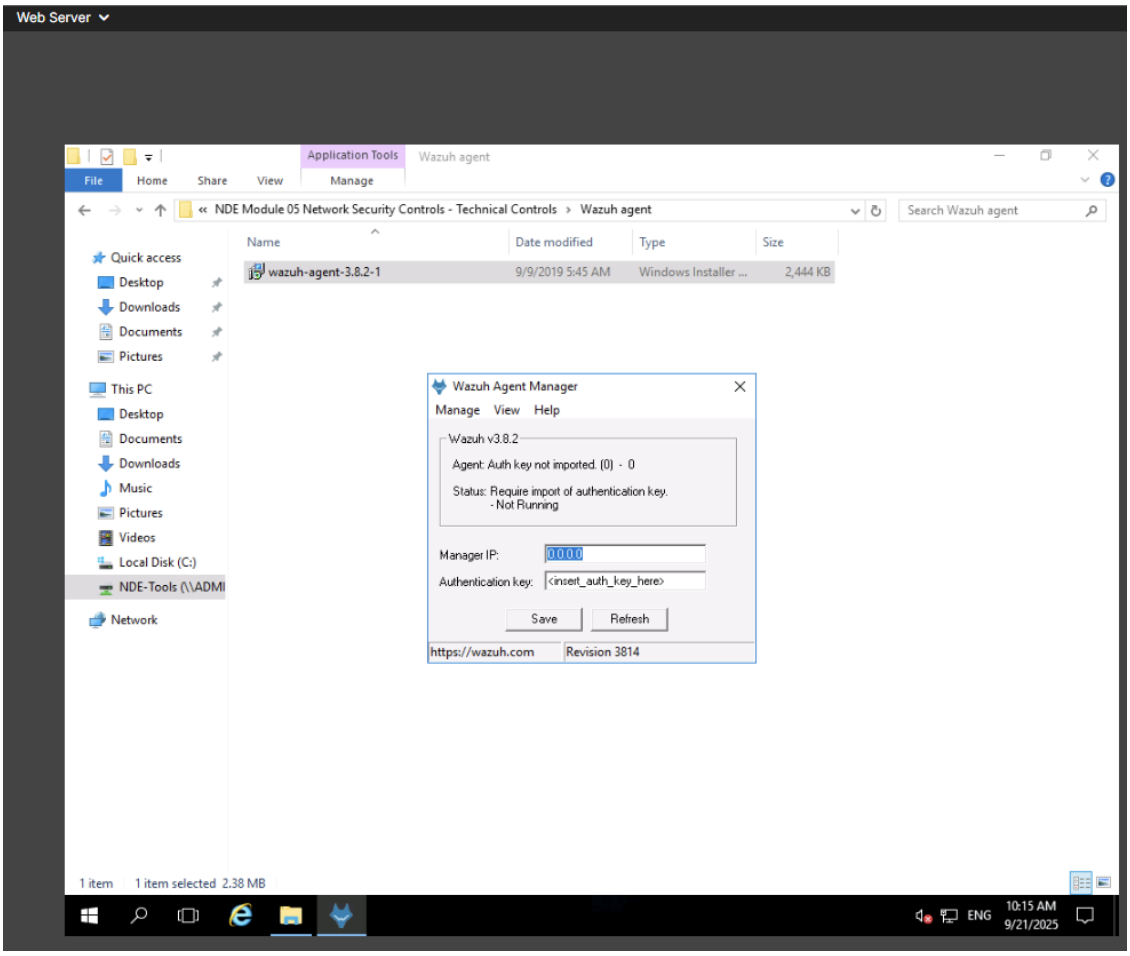

Applications Places Terminal
Sun 17:02
root@sam-Virtual-Machine: /home/sam
File Edit View Search Terminal Help
Please provide the following:
* A name for the new agent: WebServer
* The IP Address of the new agent: 10.10.1.16
Confirm adding it?(y/n): y
Agent added with ID 001.
****
* Wazuh v3.9.5 Agent manager. *
* The following options are available: *
****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: E
Available agents:
ID: 001, Name: WebServer, IP: 10.10.1.16
Provide the ID of the agent to extract the key (or '\q' to quit): Q
** Invalid ID 'Q' given. ID is not present.
Provide the ID of the agent to extract the key (or '\q' to quit): \q
****
* Wazuh v3.9.5 Agent manager. *
* The following options are available: *
****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: E
Available agents:
ID: 001, Name: WebServer, IP: 10.10.1.16
Provide the ID of the agent to extract the key (or '\q' to quit): 001
Agent key information for '001' is:
MDAxIFdlYlNlcnZlciAxMC4xMC4xLjE2IDQ5NThkM2M1NGI5ZTVkNDg5YzQ5MWJmMDJhN2NmM2I5NzI3ZjlmZGRjOGQ3YTgyM2YyNzllYTg1ZTAzNmUzYTQ=
** Press ENTER to return to the main menu.
root@sam-Virtual-Machine: /home/...
1 / 4

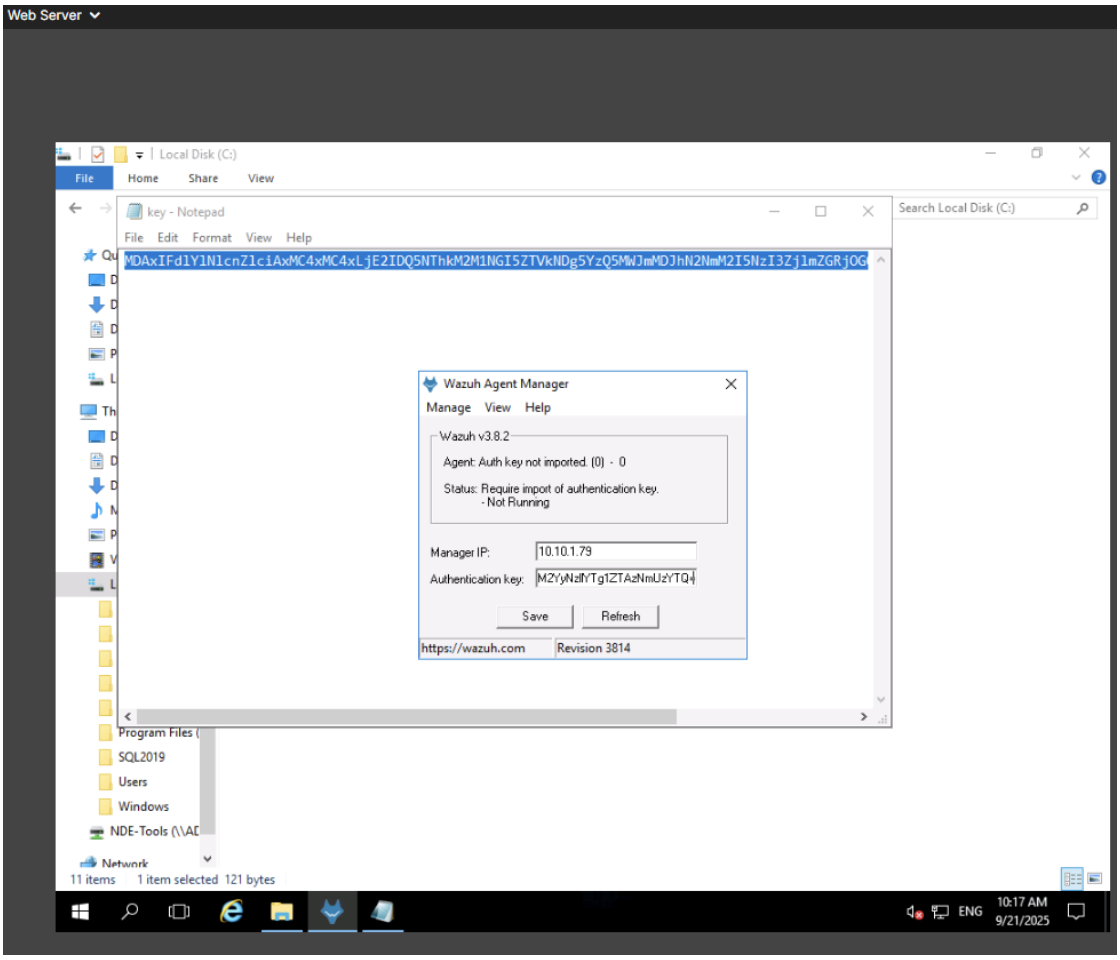

Applications Places gedit
Sun 17:04
root@sam-Virtual-Machine: /home/sam
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ sudo gedit key.txt
[sudo] password for sam:
*key.txt
Open
Save
File Edit View Search Tools Documents Help
4xLjE2IDQ5NThkM2M1NGI5ZTVkNDg5YzQ5MWJmMDJhN2NmM2I5NzI3ZjlmZGRjOGQ3YTgyM2YyNzllYTg1ZTAzNmUzYTQ=
Plain Text
Tab Width: 8
Ln 1, Col 121
INS
root@sam-Virtual-Machine: /home/...
sam@sam-Virtual-Machine: ~
1 / 4

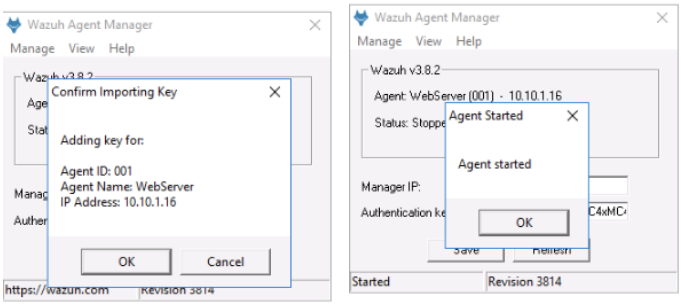

Applications
Places
Files
Sun 17:10
home
key.txt
Trash
Setup
Kibana
README
Squil
Squert
CyberChef
Home
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Network
Computer
Music
Videos
Cancel
Connect
Password required for 10.10.1.16
Username
Administrator
Domain
WORKGROUP
Password
Forget password immediately
Remember password until you logout
Remember forever
Home
1 / 4

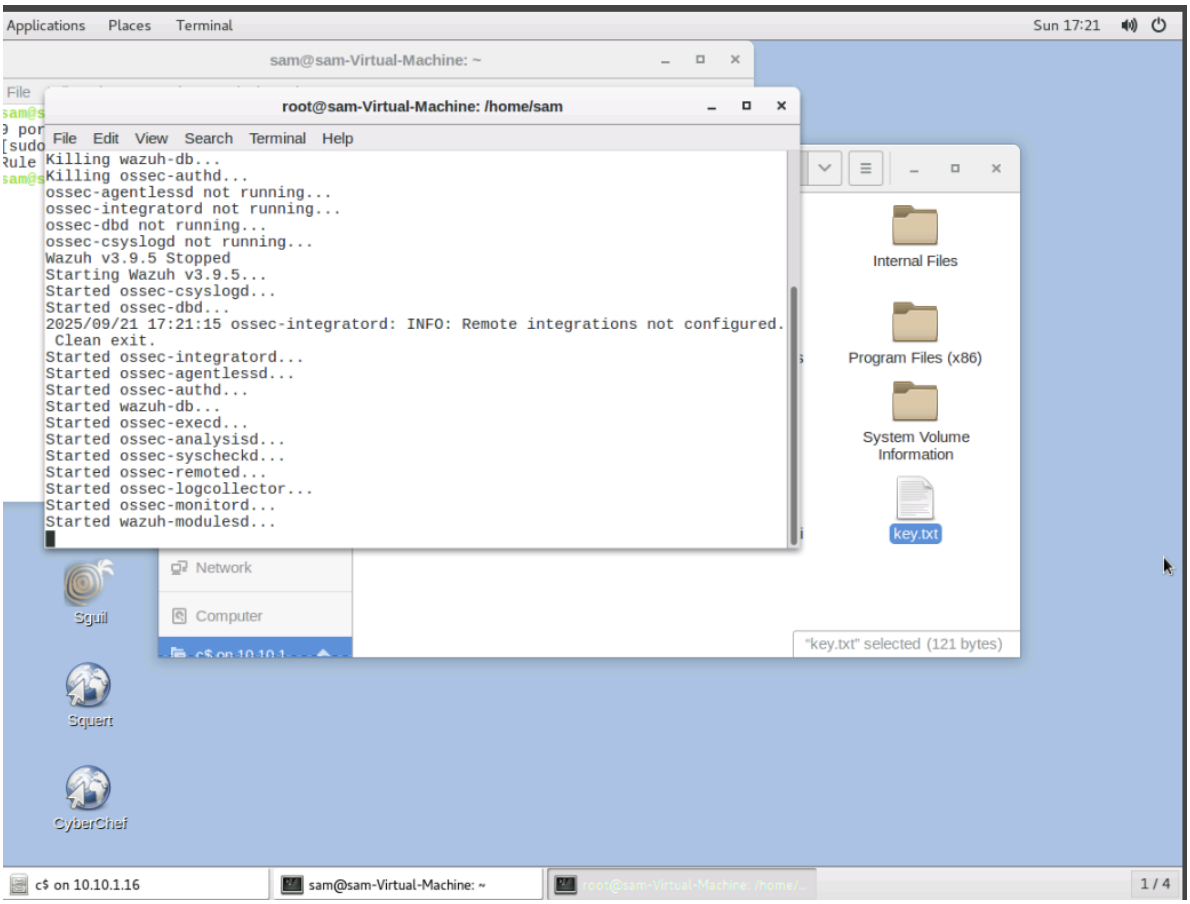

Applications
Places
Files
Sun 17:11
home
key.txt
Trash
Setup
Kibana
README
Squil
Squert
CyberChef
c$ on 10.10.1.16
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Network
Computer
DemoFTPSite
Documents and Settings
inetpub
Internal Files
PerfLogs
ProgramData
Program Files
Program Files (x86)
Recovery
$Recycle.Bin
SQL2019
System Volume Information
Users
Windows
AVScanner.ini
key.txt
"key.txt" selected (121 bytes)
1 / 4

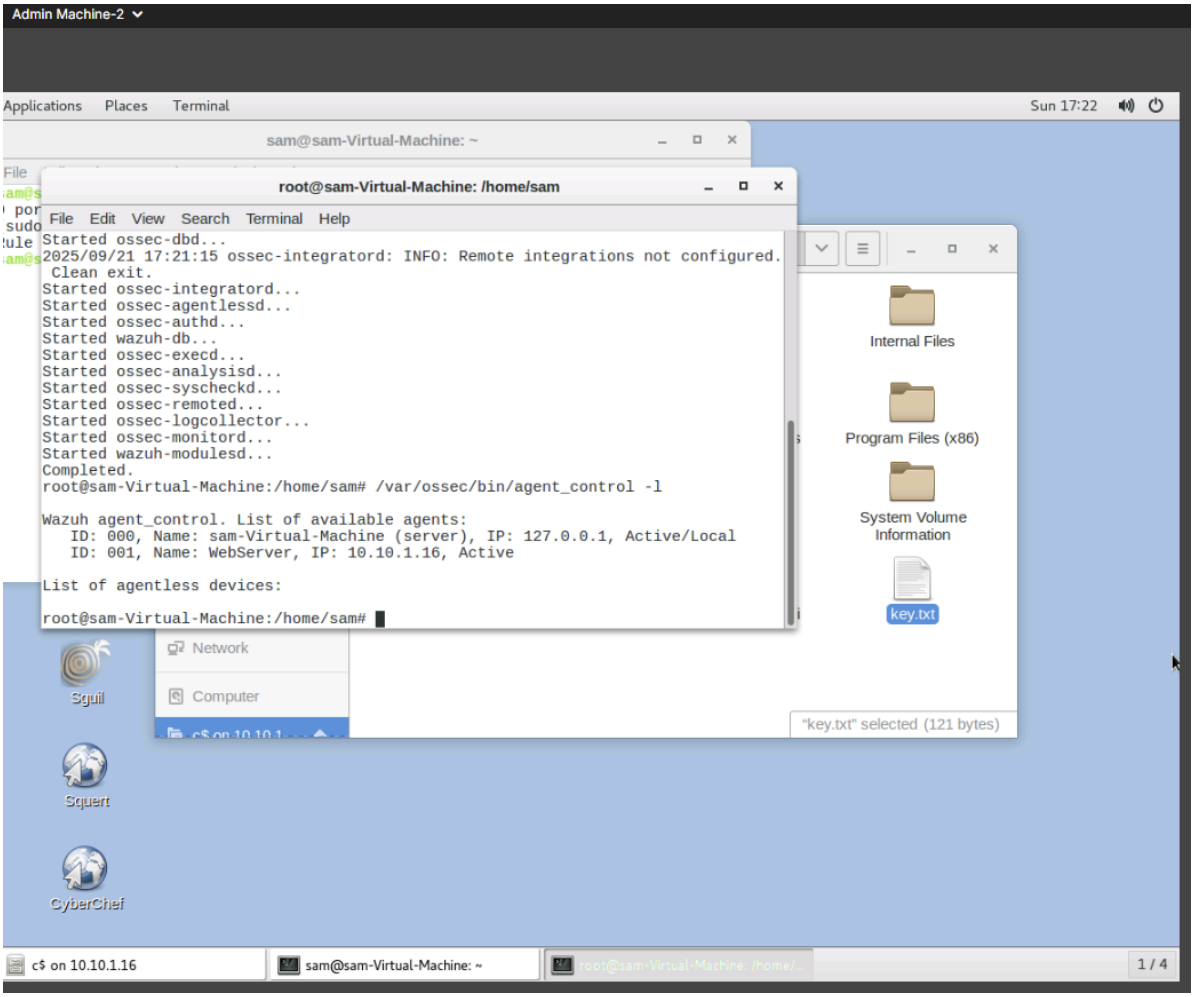

Applications
Places
Terminal
Sun 17:13
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ sudo ufw allow proto udp from 10.10.1.16 to 10.10.1.7
9 port 1514
[sudo] password for sam:
Rule added
sam@sam-Virtual-Machine:~$
Internal Files
Program Files (x86)
System Volume Information
Users
Windows
AVScanner.ini
key.txt
"key.txt" selected (121 bytes)
README
Trash
Network
Computer
Squil
Squert
CyberChef
c$ on 10.10.1.16
1 / 4

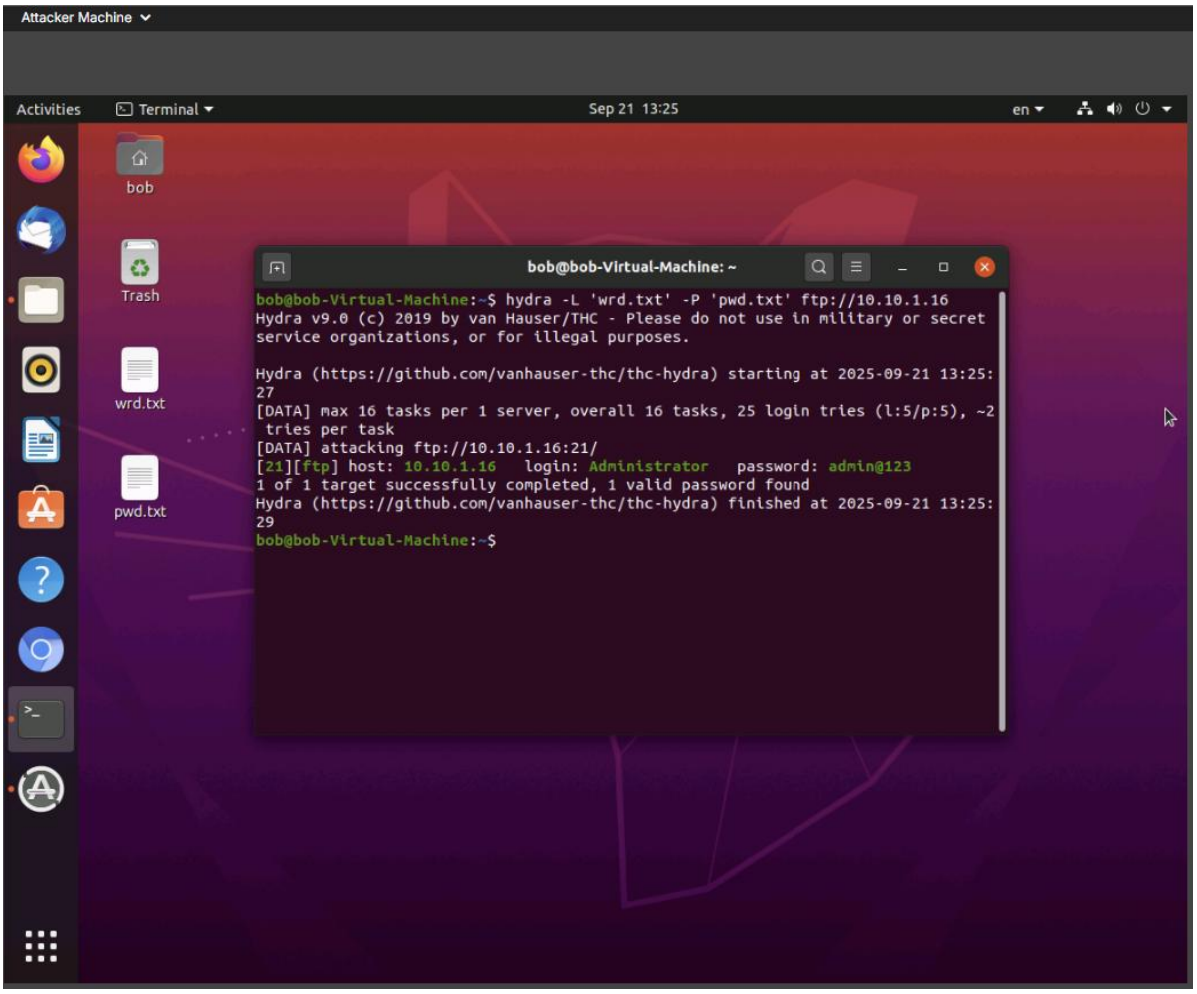

Web Server
Application Tools
Wazuh agent
File
Home
Share
View
Manage
« NDE Module 05 Network Security Controls - Technical Controls › Wazuh agent
Search Wazuh agent
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
NDE-Tools (\\ADMI
Network
Name
Date modified
Type
Size
wazuh-agent-3.8.2-1
9/9/2019 5:45 AM
Windows Installer ...
2,444 KB
Wazuh Agent Manager
Manage
View
Help
Wazuh v3.8.2
Agent: Auth key not imported. (0) - 0
Status: Require import of authentication key.
- Not Running
Manager IP:
0.0.0.0
Authentication key:
<insert_auth_key_here>
Save
Refresh
https://wazuh.com
Revision 3814
1 item
1 item selected 2.38 MB
ENG
10:15 AM
9/21/2025

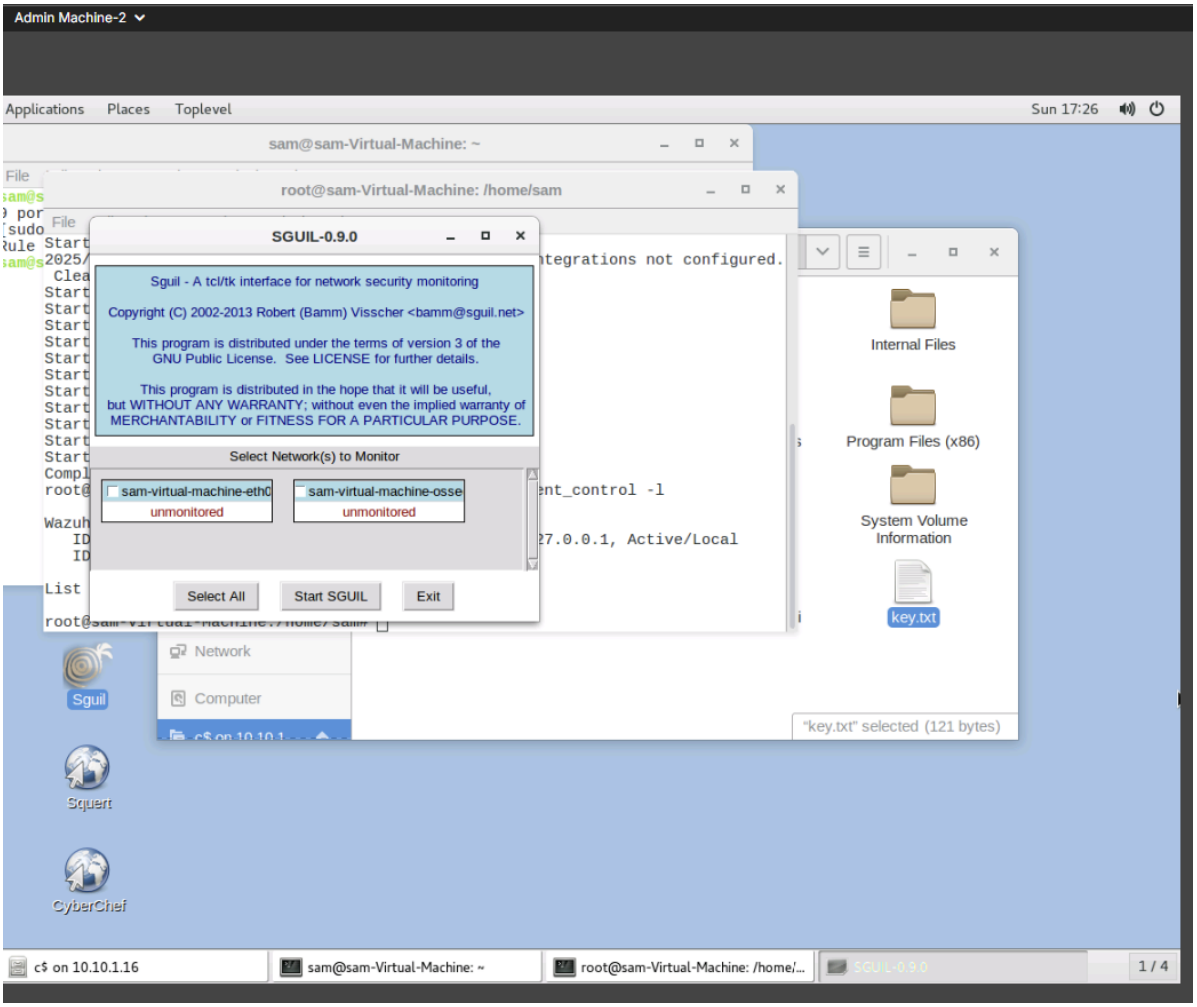

Web Server
Local Disk (C:)
File
Home
Share
View
key - Notepad
File Edit Format View Help
MDAxIFdlYlNlcnZlciAxMC4xMC4xLjE2IDQ5NThkM2M1NGI5ZTVkNDg5YzQ5MWJmMDJhN2NmM2I5NzI3ZjlmZGRjOG
Search Local Disk (C:)
Wazuh Agent Manager
Manage View Help
Wazuh v3.8.2
Agent: Auth key not imported. (0) - 0
Status: Require import of authentication key.
- Not Running
Manager IP:
10.10.1.79
Authentication key:
M2YyNzlfYTg1ZTAzNmUzYTQ4
Save
Refresh
https://wazuh.com
Revision 3814
Program Files
SQL2019
Users
Windows
NDE-Tools (\\AD
Network
11 items
1 item selected 121 bytes
ENG
10:17 AM
9/21/2025

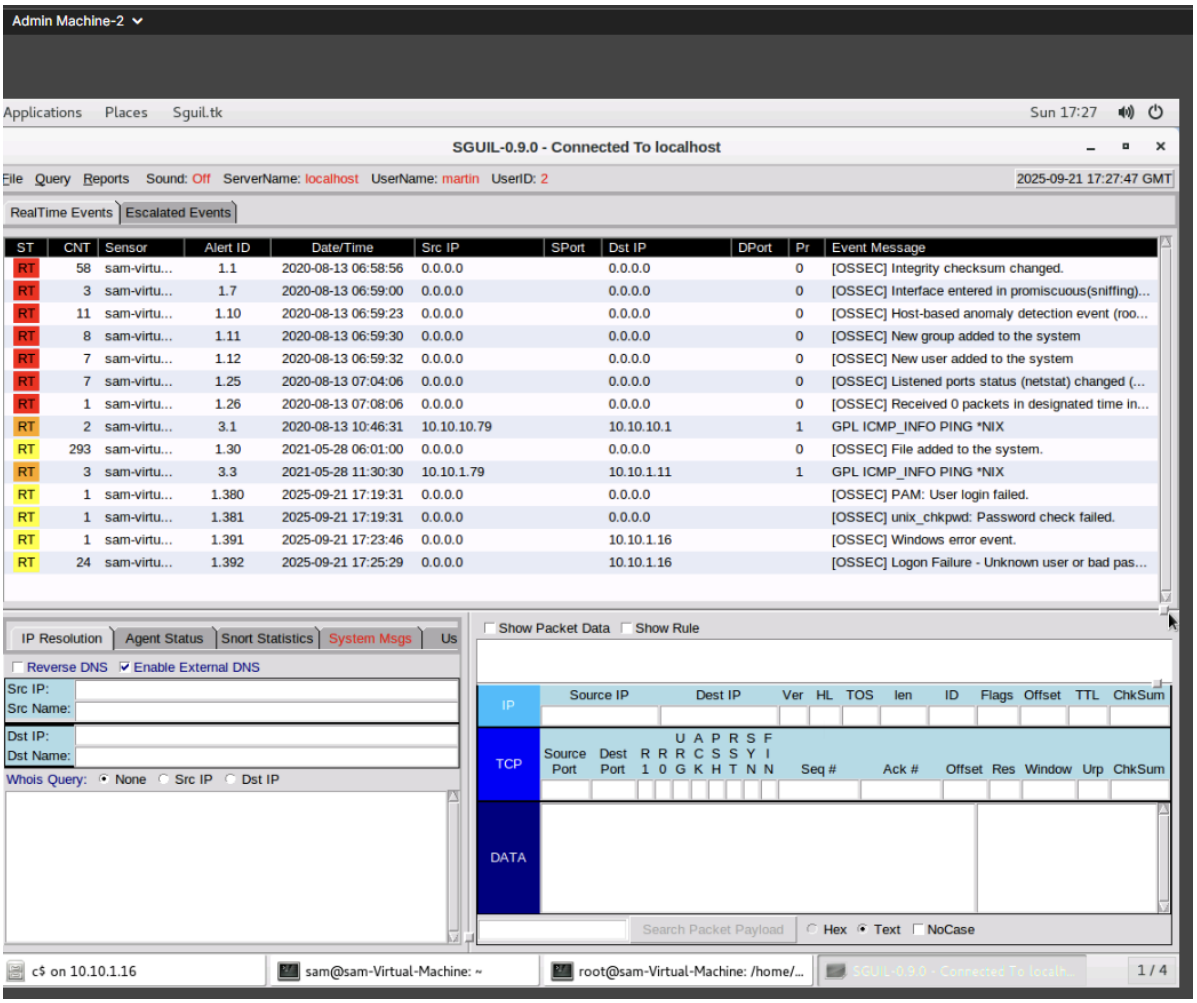

Wazuh Agent Manager
Manage View Help
Confirm Importing Key
Adding key for:
Agent ID: 001
Agent Name: WebServer
IP Address: 10.10.1.16
OK
Cancel
Wazuh Agent Manager
Manage View Help
Wazuh v3.8.2
Agent: WebServer (001) - 10.10.1.16
Agent Started
Agent started
OK
Manager IP:
Started
Revision 3814

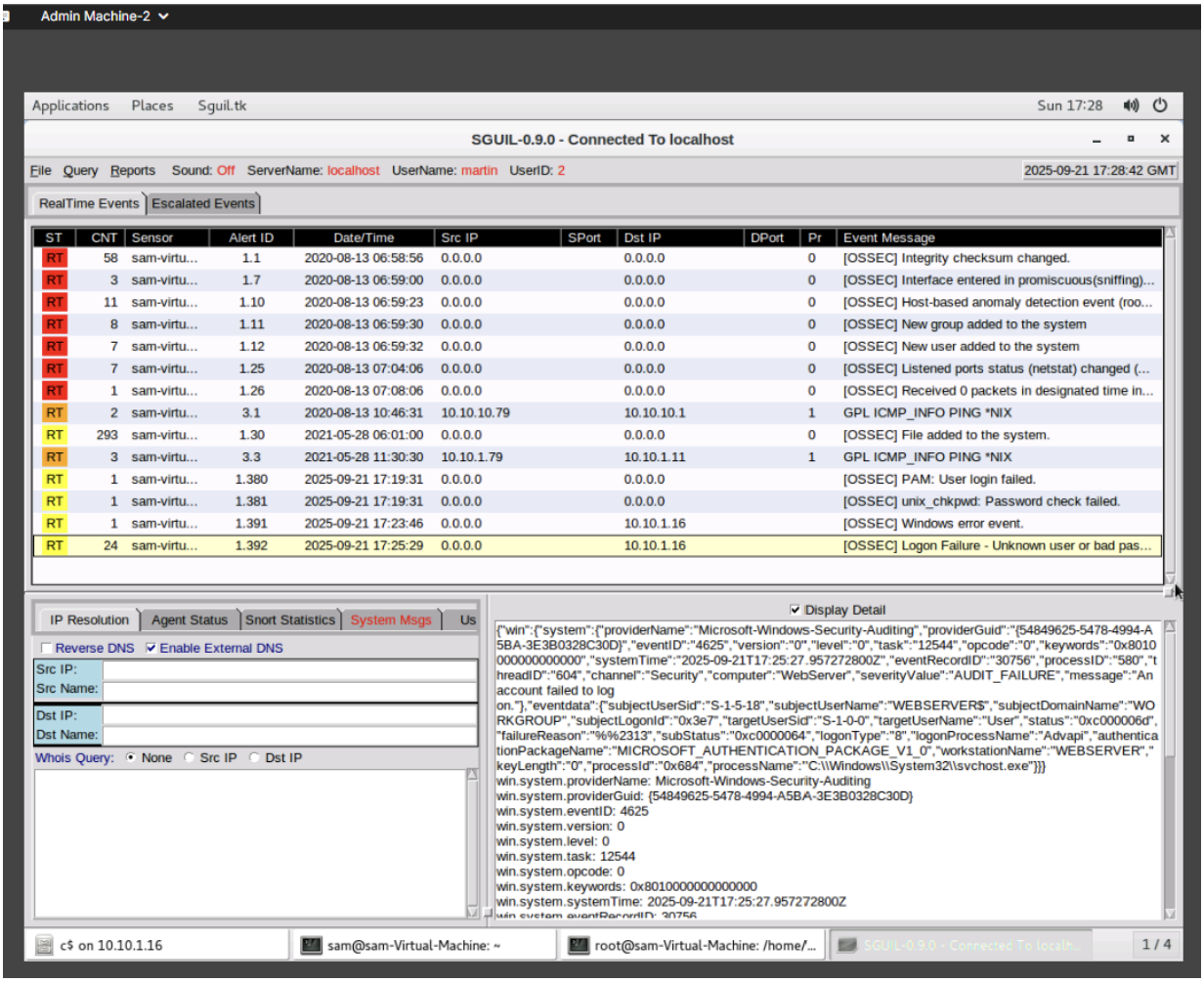

Applications Places Terminal
Sun 17:21
sam@sam-Virtual-Machine: ~
root@sam-Virtual-Machine: /home/sam
File Edit View Search Terminal Help
Killing wazuh-db...
Killing ossec-authd...
ossec-agentlessd not running...
ossec-integratord not running...
ossec-dbd not running...
ossec-csyslogd not running...
Wazuh v3.9.5 Stopped
Starting Wazuh v3.9.5...
Started ossec-csyslogd...
Started ossec-dbd...
2025/09/21 17:21:15 ossec-integratord: INFO: Remote integrations not configured.
Clean exit.
Started ossec-integratord...
Started ossec-agentlessd...
Started ossec-authd...
Started wazuh-db...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-syscheckd...
Started ossec-remoted...
Started ossec-logcollector...
Started ossec-monitord...
Started wazuh-modulesd...
Internal Files
Program Files (x86)
System Volume Information
key.txt
Network
Computer
"key.txt" selected (121 bytes)
Sguil
Squert
CyberChef
c$ on 10.10.1.16
sam@sam-Virtual-Machine: ~
1 / 4


Admin Machine-2
Applications
Places
Terminal
Sun 17:22
sam@sam-Virtual-Machine: ~
root@sam-Virtual-Machine: /home/sam
File Edit View Search Terminal Help
Started ossec-dbd...
2025/09/21 17:21:15 ossec-integratord: INFO: Remote integrations not configured.
Clean exit.
Started ossec-integratord...
Started ossec-agentlessd...
Started ossec-authd...
Started wazuh-db...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-syscheckd...
Started ossec-remoted...
Started ossec-logcollector...
Started ossec-monitord...
Started wazuh-modulesd...
Completed.
root@sam-Virtual-Machine:/home/sam# /var/ossec/bin/agent_control -l
Wazuh agent_control. List of available agents:
ID: 000, Name: sam-Virtual-Machine (server), IP: 127.0.0.1, Active/Local
ID: 001, Name: WebServer, IP: 10.10.1.16, Active
List of agentless devices:
root@sam-Virtual-Machine:/home/sam#
Internal Files
Program Files (x86)
System Volume Information
key.txt
Network
Computer
"key.txt" selected (121 bytes)
Sguil
Squert
CyberChef
c$ on 10.10.1.16
sam@sam-Virtual-Machine: ~
1 / 4


Attacker Machine
Activities
Terminal
Sep 21 13:25
en
bob
Trash
wrd.txt
pwd.txt
bob@bob-Virtual-Machine: ~
bob@bob-Virtual-Machine:~$ hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-21 13:25:27
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ftp://10.10.1.16:21/
[21][ftp] host: 10.10.1.16 login: Administrator password: admin@123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-21 13:25:29
bob@bob-Virtual-Machine:~$


Admin Machine-2
Applications
Places
Toplevel
Sun 17:26
sam@sam-Virtual-Machine: ~
root@sam-Virtual-Machine: /home/sam
SGUIL-0.9.0
Sguil - A tcl/tk interface for network security monitoring
Copyright (C) 2002-2013 Robert (Bamm) Visscher <bamm@sguil.net>
This program is distributed under the terms of version 3 of the GNU Public License. See LICENSE for further details.
This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Select Network(s) to Monitor
sam-virtual-machine-eth0
unmonitored
sam-virtual-machine-osse
unmonitored
Select All
Start SGUIL
Exit
Internal Files
Program Files (x86)
System Volume Information
key.txt
"key.txt" selected (121 bytes)
Network
Computer
Sguil
Squert
CyberChef
c$ on 10.10.1.16
sam@sam-Virtual-Machine: ~
root@sam-Virtual-Machine: /home/...
SGUIL-0.9.0
1 / 4


Admin Machine-2
Applications Places Sguil.tk Sun 17:27
SGUIL-0.9.0 - Connected To localhost
File Query Reports Sound: Off ServerName: localhost UserName: martin UserID: 2
2025-09-21 17:27:47 GMT
RealTime Events Escalated Events
ST CNT Sensor Alert ID Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 58 sam-virtu... 1.1 2020-08-13 06:58:56 0.0.0.0 0.0.0.0 0 [OSSEC] Integrity checksum changed.
RT 3 sam-virtu... 1.7 2020-08-13 06:59:00 0.0.0.0 0.0.0.0 0 [OSSEC] Interface entered in promiscuous(sniffing)...
RT 11 sam-virtu... 1.10 2020-08-13 06:59:23 0.0.0.0 0.0.0.0 0 [OSSEC] Host-based anomaly detection event (roo...
RT 8 sam-virtu... 1.11 2020-08-13 06:59:30 0.0.0.0 0.0.0.0 0 [OSSEC] New group added to the system
RT 7 sam-virtu... 1.12 2020-08-13 06:59:32 0.0.0.0 0.0.0.0 0 [OSSEC] New user added to the system
RT 7 sam-virtu... 1.25 2020-08-13 07:04:06 0.0.0.0 0.0.0.0 0 [OSSEC] Listened ports status (netstat) changed (...
RT 1 sam-virtu... 1.26 2020-08-13 07:08:06 0.0.0.0 0.0.0.0 0 [OSSEC] Received 0 packets in designated time in...
RT 2 sam-virtu... 3.1 2020-08-13 10:46:31 10.10.10.79 10.10.10.1 1 GPL ICMP_INFO PING *NIX
RT 293 sam-virtu... 1.30 2021-05-28 06:01:00 0.0.0.0 0.0.0.0 0 [OSSEC] File added to the system.
RT 3 sam-virtu... 3.3 2021-05-28 11:30:30 10.10.1.79 10.10.1.11 1 GPL ICMP_INFO PING *NIX
RT 1 sam-virtu... 1.380 2025-09-21 17:19:31 0.0.0.0 0.0.0.0 [OSSEC] PAM: User login failed.
RT 1 sam-virtu... 1.381 2025-09-21 17:19:31 0.0.0.0 0.0.0.0 [OSSEC] unix_chkpwd: Password check failed.
RT 1 sam-virtu... 1.391 2025-09-21 17:23:46 0.0.0.0 10.10.1.16 [OSSEC] Windows error event.
RT 24 sam-virtu... 1.392 2025-09-21 17:25:29 0.0.0.0 10.10.1.16 [OSSEC] Logon Failure - Unknown user or bad pas...
IP Resolution Agent Status Snort Statistics System Msgs Us
Reverse DNS Enable External DNS
Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query: None Src IP Dst IP
Show Packet Data Show Rule
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
TCP Source Port Dest Port R 1 R 0 U R G A C K P S H R S T S Y N F I N Seq # Ack # Offset Res Window Urp ChkSum
DATA
Search Packet Payload Hex Text NoCase
c$ on 10.10.1.16
sam@sam-Virtual-Machine: ~
root@sam-Virtual-Machine: /home/...
SGUIL-0.9.0 - Connected To localh...
1 / 4



Exercise 6: Implementing Network-Based IDS Functionality using Suricata IDS

Real-time Intrusion Detection is a requirement for today's networks. With the help of various tools and techniques, it is possible identifying known and potentially harmful attacks.

Lab Scenario

Network defenders can use Suricata for real-time Intrusion Detection System (IDS), inline Intrusion Prevention System (IPS), Network Security Monitoring (NSM), and offline pcap processing.

Lab Objectives

This lab will demonstrate how to use Suricata IDS.

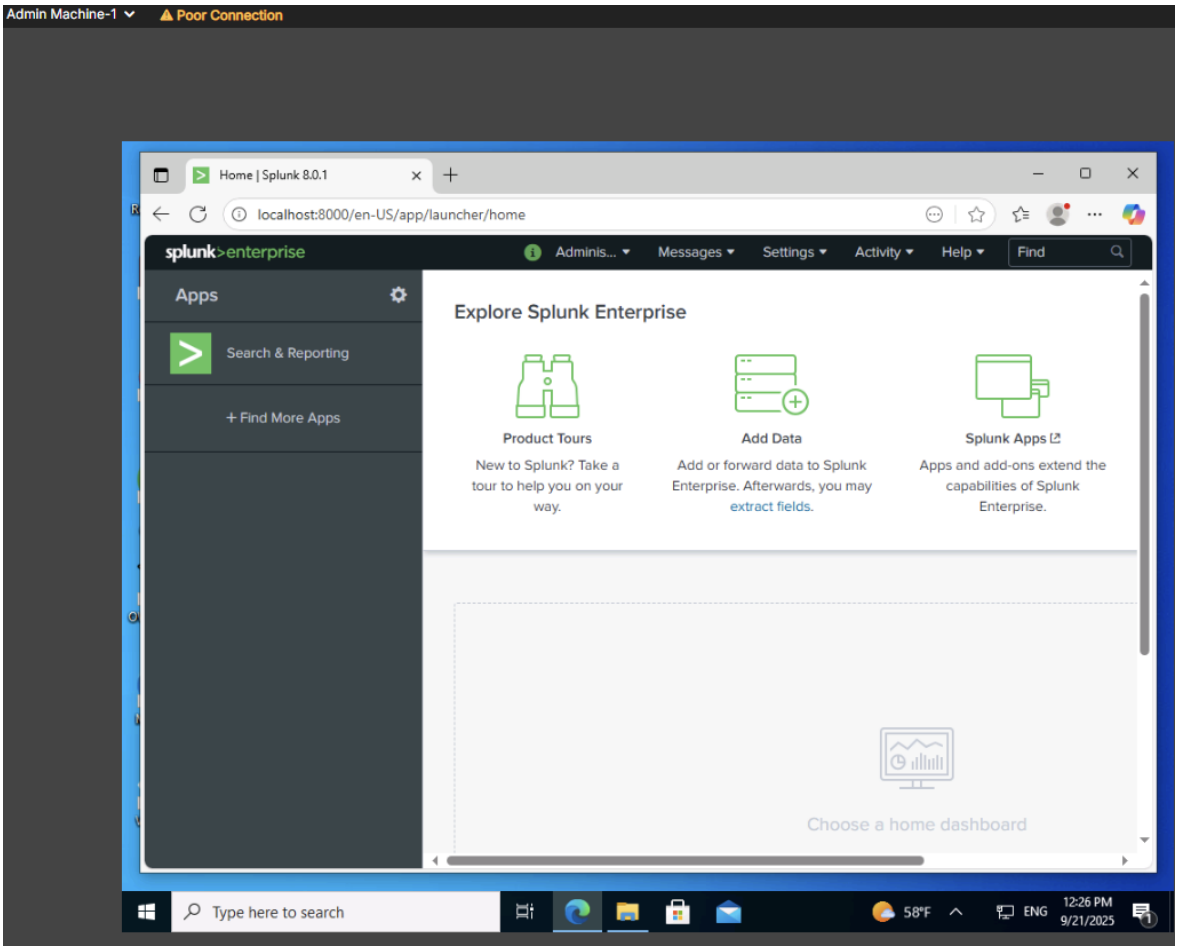
In this lab, you will learn how to:

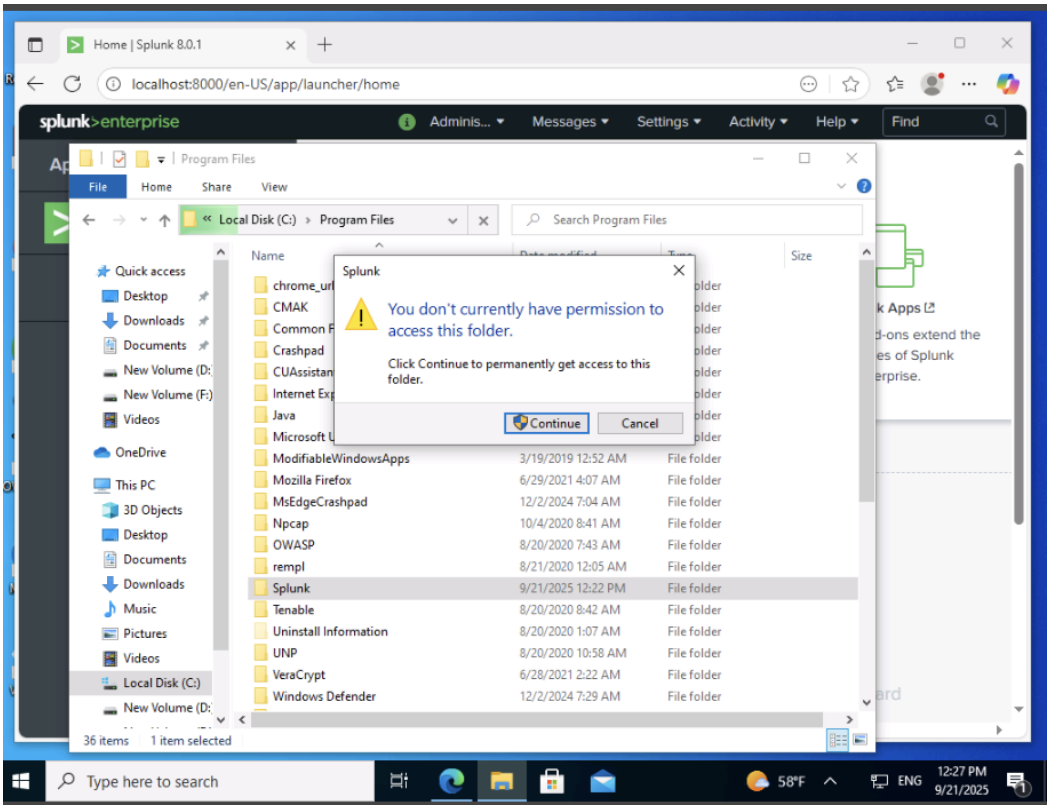
- Use the intrusion detection tool Suricata

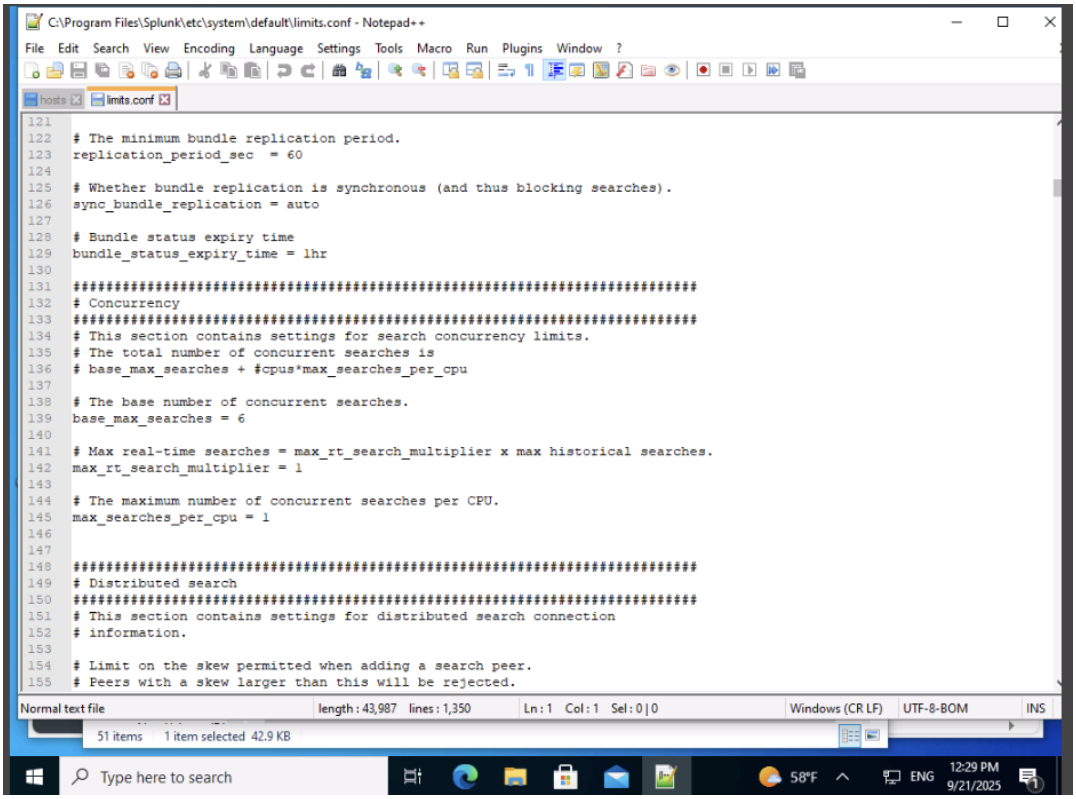
- Review information in the Suricata Logs.

Overview of Suricata IDS

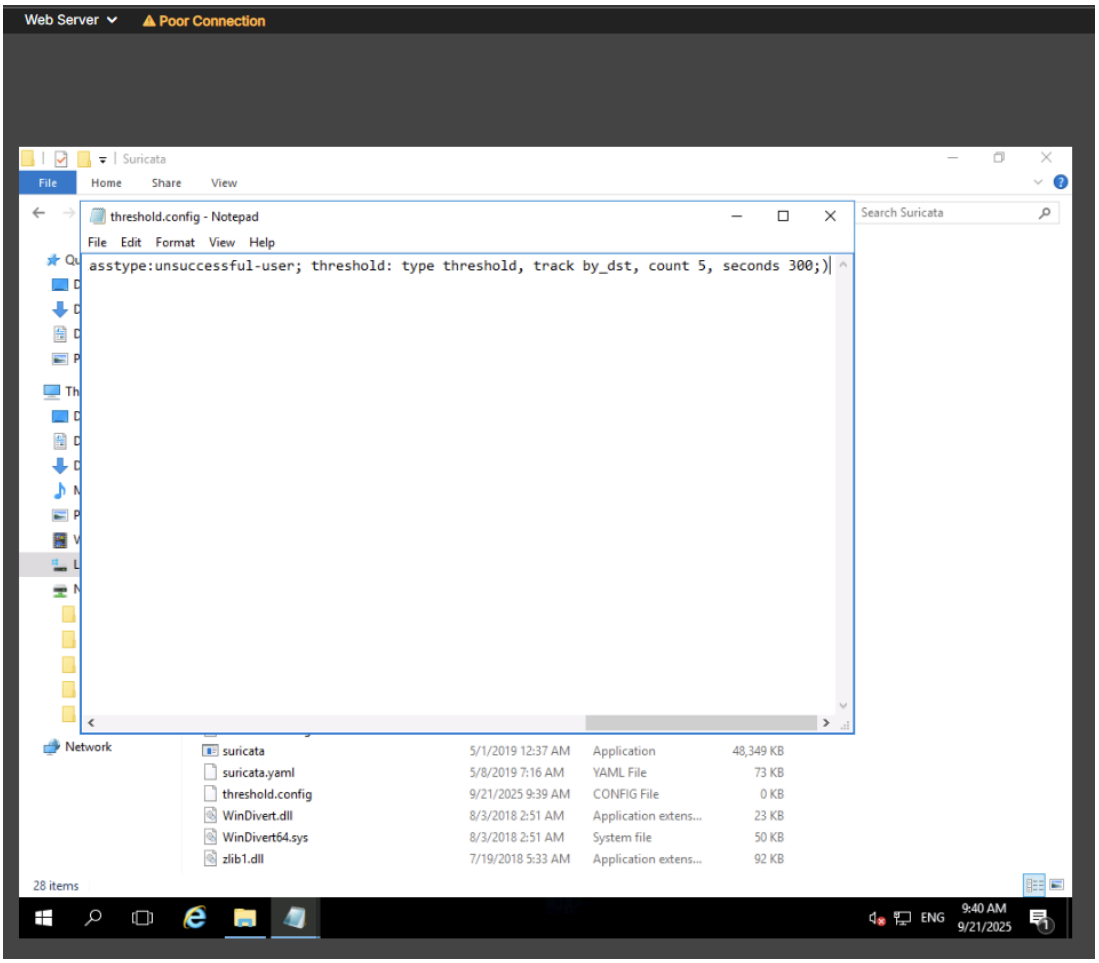
Suricata is an open-source network intrusion prevention system. It is a fast and robust network threat detection engine. Suricata uses rules and signature language for inspecting network traffic. The IDS performs intrusion detection and attempts to stop detected incidents. Suricata supports standard input-output formats such as YAML and JSON, which can be easily integrated with various SIEM tools like Splunk, Logstash/Elasticsearch, and Kibana.

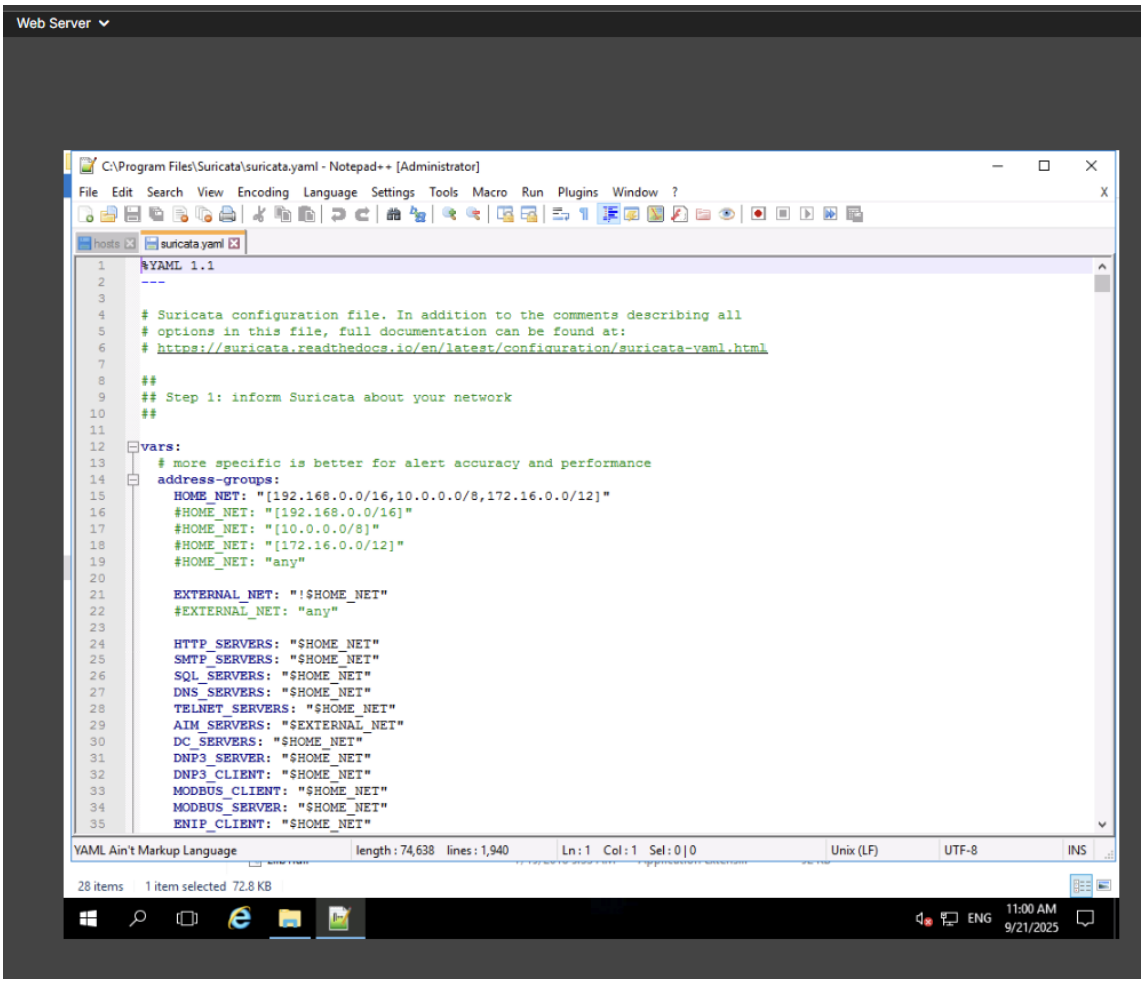



Home | Splunk 8.0.1
localhost:8000/en-US/app/launcher/home
splunk>enterprise
Adminis...
Messages
Settings
Activity
Help
Find
Program Files
File
Home
Share
View
Local Disk (C:) › Program Files
Search Program Files
Quick access
Desktop
Downloads
Documents
New Volume (D:
New Volume (F:)
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:
Name
Size
chrome_url
CMAK
Common F
Crashpad
CUAssistan
Internet Exp
Java
Microsoft U
ModifiableWindowsApps 3/19/2019 12:52 AM File folder
Mozilla Firefox 6/29/2021 4:07 AM File folder
MsEdgeCrashpad 12/2/2024 7:04 AM File folder
Npcap 10/4/2020 8:41 AM File folder
OWASP 8/20/2020 7:43 AM File folder
rempl 8/21/2020 12:05 AM File folder
Splunk 9/21/2025 12:22 PM File folder
Tenable 8/20/2020 8:42 AM File folder
Uninstall Information 8/20/2020 1:07 AM File folder
UNP 8/20/2020 10:58 AM File folder
VeraCrypt 6/28/2021 2:22 AM File folder
Windows Defender 12/2/2024 7:29 AM File folder
Splunk
You don't currently have permission to access this folder.
Click Continue to permanently get access to this folder.
Continue
Cancel
36 items
1 item selected
Type here to search
58°F
ENG
12:27 PM
9/21/2025

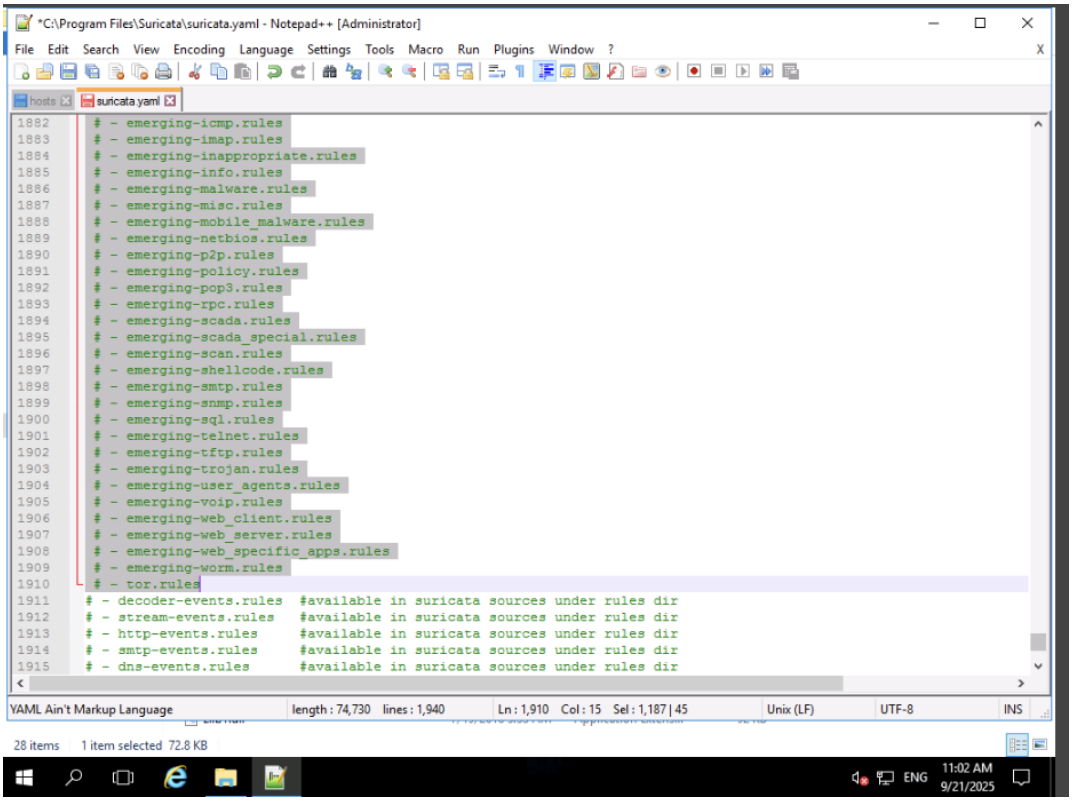

C:\Program Files\Splunk\etc\system\default\limits.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts
limits.conf
# The minimum bundle replication period.
replication_period_sec = 60
# Whether bundle replication is synchronous (and thus blocking searches).
sync_bundle_replication = auto
# Bundle status expiry time
bundle_status_expiry_time = 1hr
# Concurrency
# This section contains settings for search concurrency limits.
# The total number of concurrent searches is
# base_max_searches + #cpus*max_searches_per_cpu
# The base number of concurrent searches.
base_max_searches = 6
# Max real-time searches = max_rt_search_multiplier x max historical searches.
max_rt_search_multiplier = 1
# The maximum number of concurrent searches per CPU.
max_searches_per_cpu = 1
# Distributed search
# This section contains settings for distributed search connection
# information.
# Limit on the skew permitted when adding a search peer.
# Peers with a skew larger than this will be rejected.
Normal text file
length : 43,987 lines : 1,350
Ln : 1 Col : 1 Sel : 0 | 0
Windows (CR LF)
UTF-8-BOM
INS
51 items
1 item selected 42.9 KB
Type here to search
58°F
ENG
12:29 PM
9/21/2025

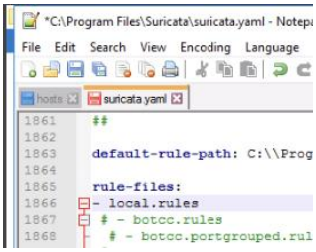
```
# The maximum number of concurrent
max_searches_per_cpu = 2
```

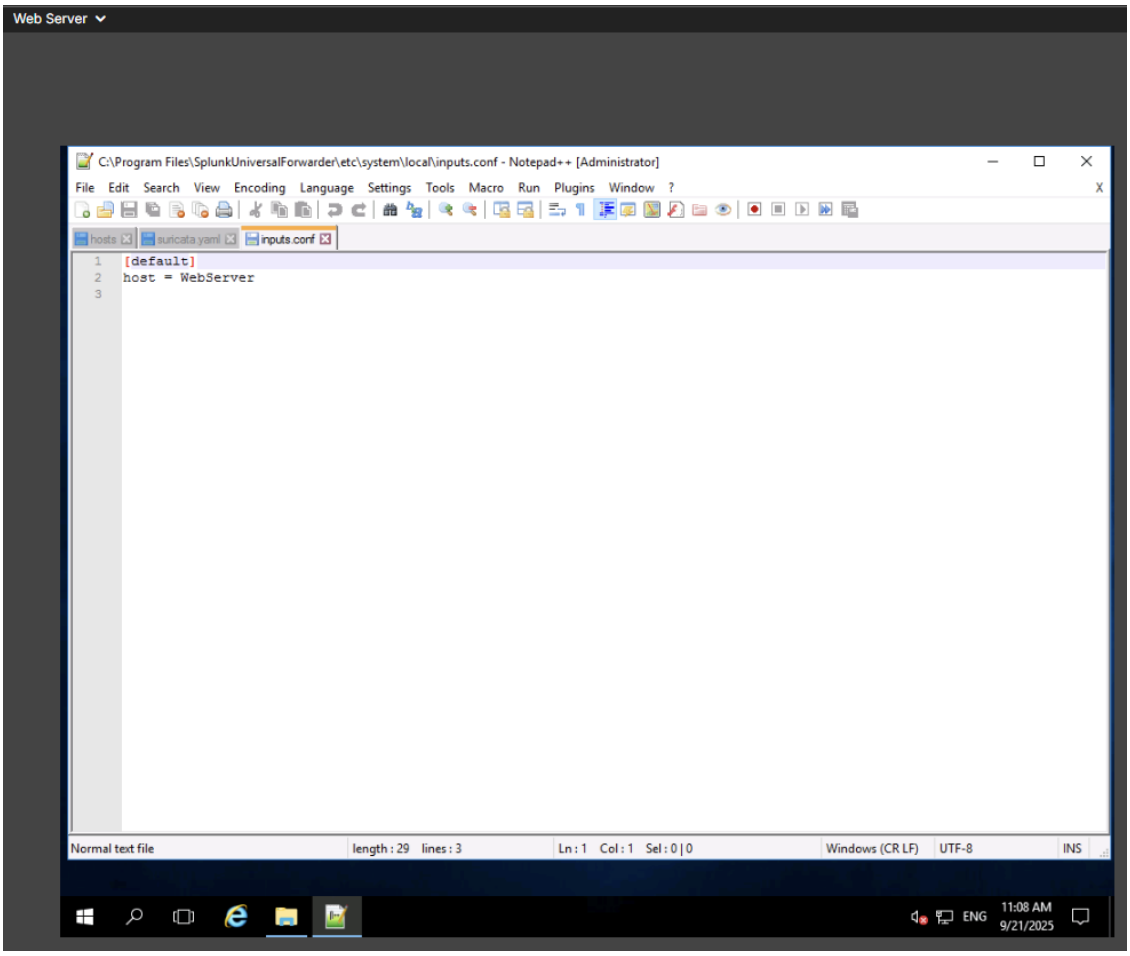


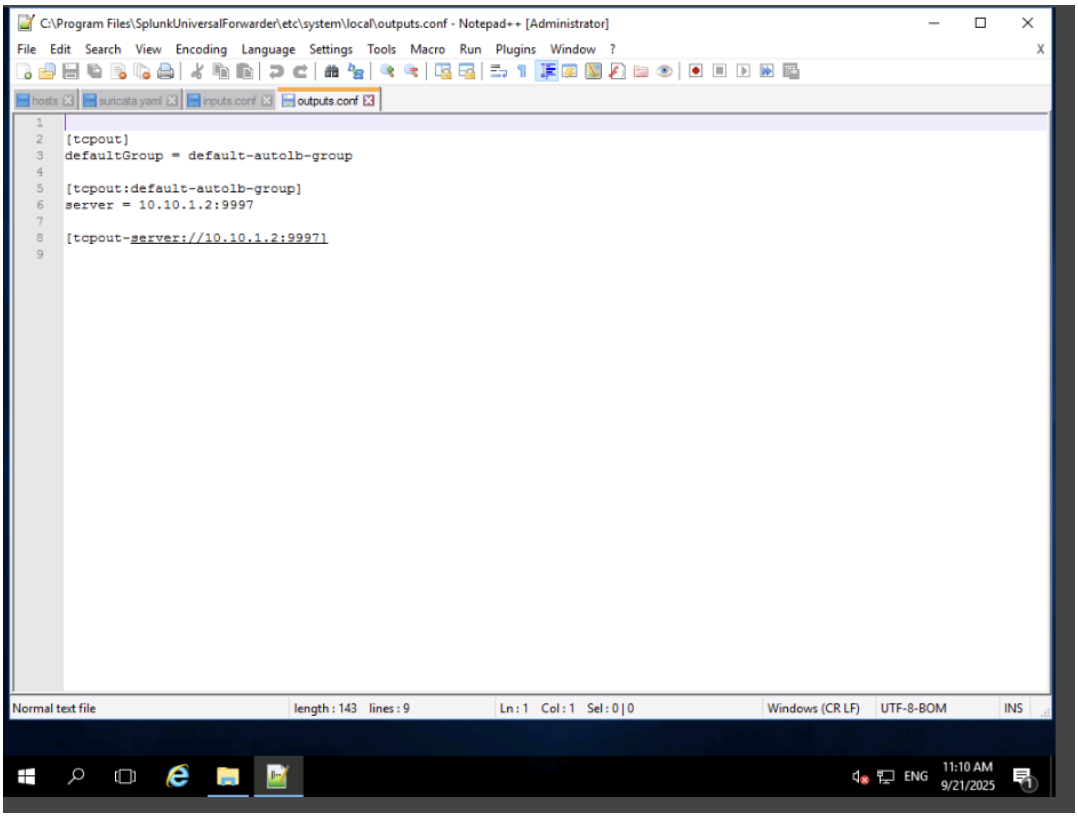

Web Server
C:\Program Files\Suricata\suricata.yaml - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts
suricata.yaml
%YAML 1.1

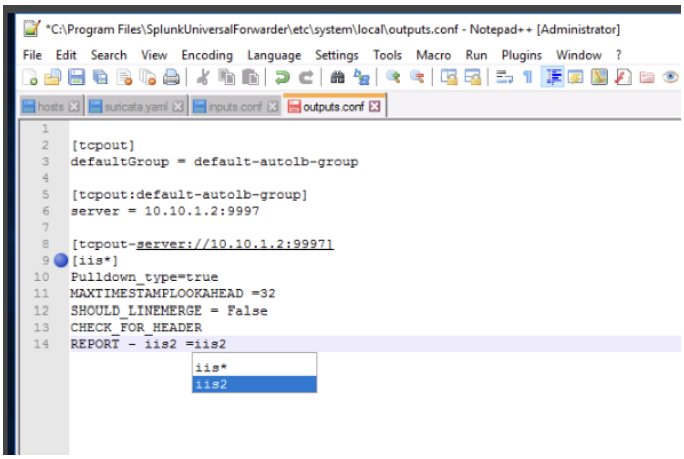
Suricata configuration file. In addition to the comments describing all
options in this file, full documentation can be found at:
https://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html
##
Step 1: inform Suricata about your network
##
vars:
more specific is better for alert accuracy and performance
address-groups:
HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
#HOME_NET: "[192.168.0.0/16]"
#HOME_NET: "[10.0.0.0/8]"
#HOME_NET: "[172.16.0.0/12]"
#HOME_NET: "any"
EXTERNAL_NET: "!$HOME_NET"
#EXTERNAL_NET: "any"
HTTP_SERVERS: "$HOME_NET"
SMTP_SERVERS: "$HOME_NET"
SQL_SERVERS: "$HOME_NET"
DNS_SERVERS: "$HOME_NET"
TELNET_SERVERS: "$HOME_NET"
AIM_SERVERS: "$EXTERNAL_NET"
DC_SERVERS: "$HOME_NET"
DNP3_SERVER: "$HOME_NET"
DNP3_CLIENT: "$HOME_NET"
MODBUS_CLIENT: "$HOME_NET"
MODBUS_SERVER: "$HOME_NET"
ENIP_CLIENT: "$HOME_NET"
YAML Ain't Markup Language
length : 74,638 lines : 1,940
Ln : 1 Col : 1 Sel : 0 | 0
Unix (LF)
UTF-8
INS
28 items
1 item selected 72.8 KB
ENG
11:00 AM
9/21/2025

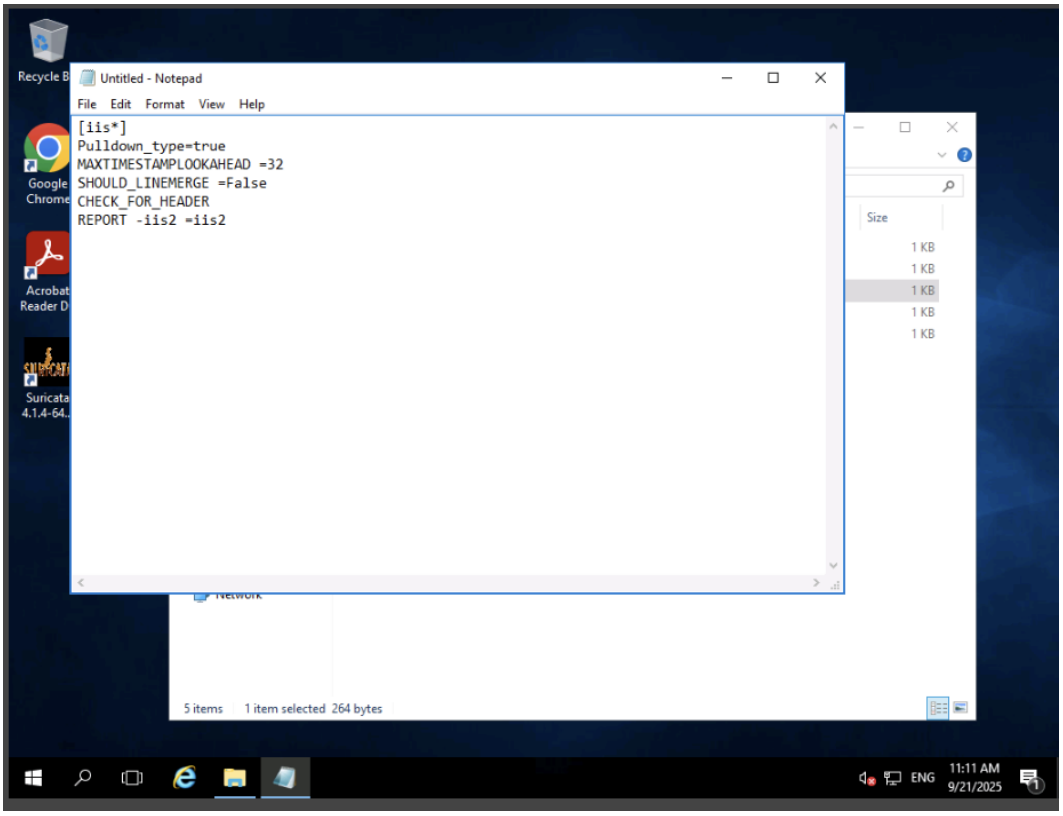

*C:\Program Files\Suricata\suricata.yaml - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts
suricata.yaml
- emerging-icmp.rules
- emerging-imap.rules
- emerging-inappropriate.rules
- emerging-info.rules
- emerging-malware.rules
- emerging-misc.rules
- emerging-mobile_malware.rules
- emerging-netbios.rules
- emerging-p2p.rules
- emerging-policy.rules
- emerging-pop3.rules
- emerging-rpc.rules
- emerging-scada.rules
- emerging-scada_special.rules
- emerging-scan.rules
- emerging-shellcode.rules
- emerging-smtp.rules
- emerging-snmp.rules
- emerging-sql.rules
- emerging-telnet.rules
- emerging-tftp.rules
- emerging-trojan.rules
- emerging-user_agents.rules
- emerging-voip.rules
- emerging-web_client.rules
- emerging-web_server.rules
- emerging-web_specific_apps.rules
- emerging-worm.rules
- tor.rules
- decoder-events.rules #available in suricata sources under rules dir
- stream-events.rules #available in suricata sources under rules dir
- http-events.rules #available in suricata sources under rules dir
- smtp-events.rules #available in suricata sources under rules dir
- dns-events.rules #available in suricata sources under rules dir
YAML Ain't Markup Language
length : 74,730 lines : 1,940
Ln : 1,910 Col : 15 Sel : 1,187 | 45
Unix (LF)
UTF-8
INS
28 items
1 item selected 72.8 KB
ENG
11:02 AM
9/21/2025

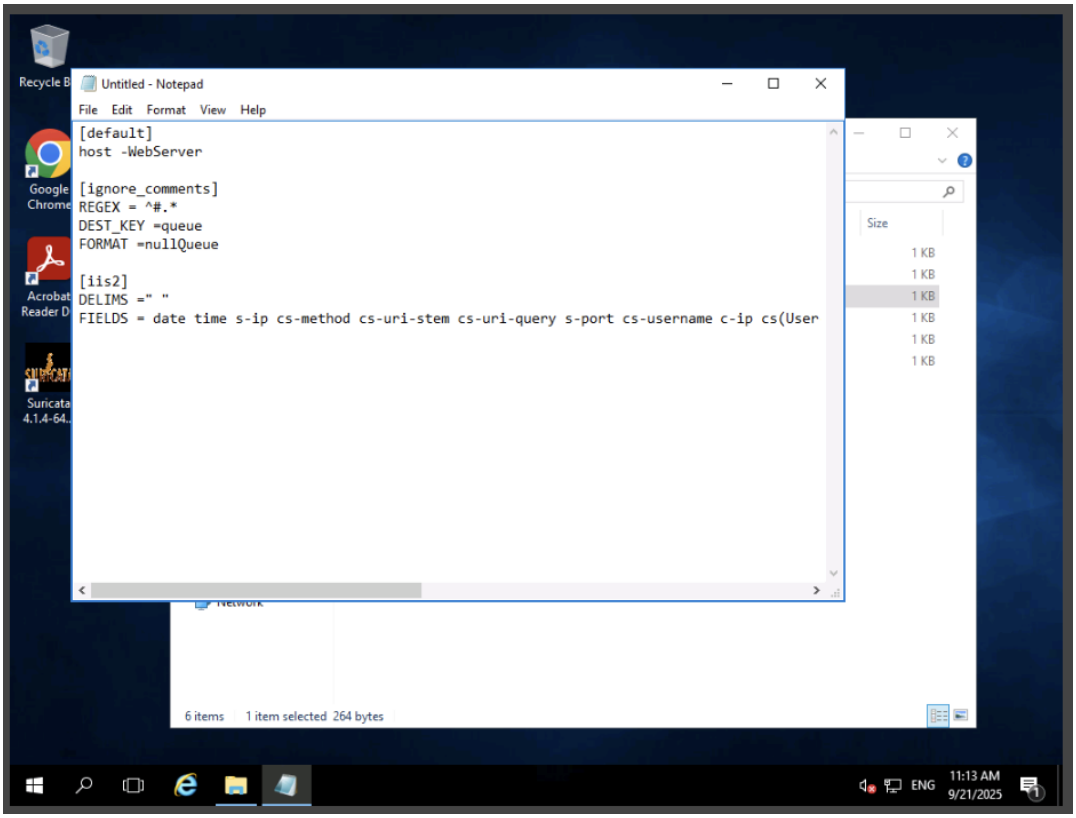

*C:\Program Files\Suricata\suricata.yaml - Notepa
File Edit Search View Encoding Language
hosts
suricata.yaml
##
default-rule-path: C:\\Prog
rule-files:
- local.rules
- botcc.rules
- botcc.portgrouped.rul

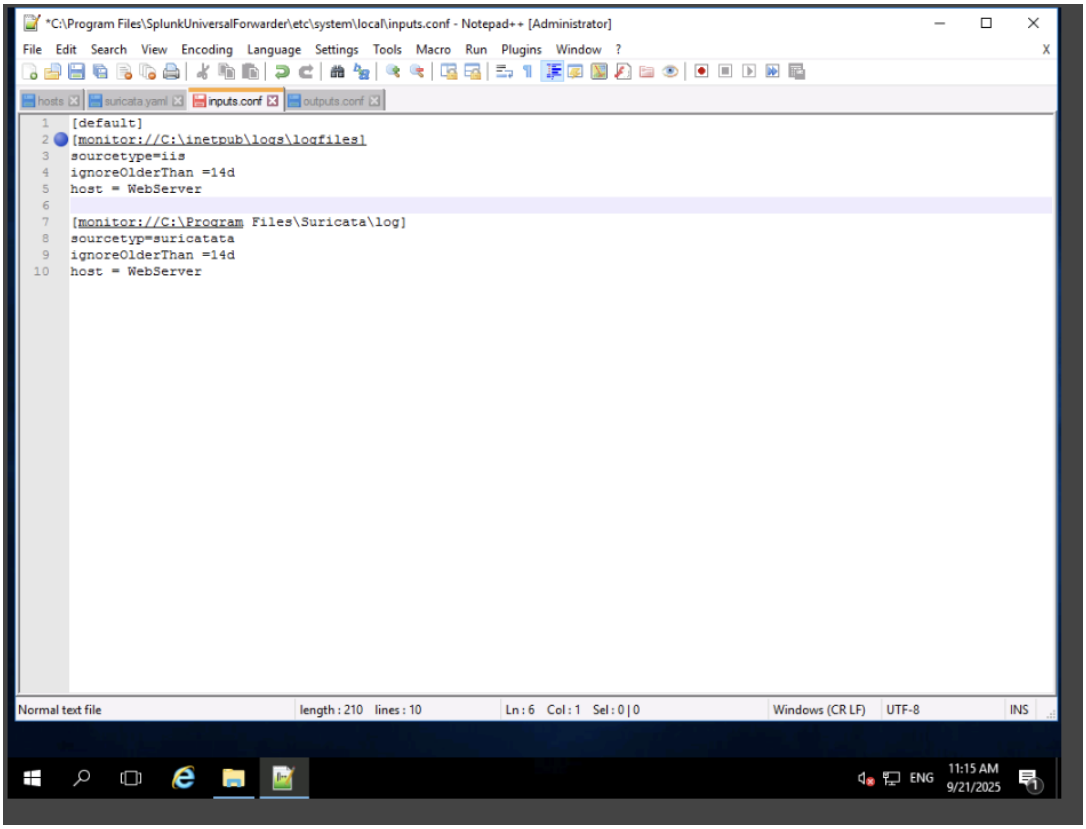

Web Server
C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts
suricata.yaml
inputs.conf
1 [default]
2 host = WebServer
3
Normal text file
length : 29 lines : 3
Ln : 1 Col : 1 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS
ENG
11:08 AM
9/21/2025

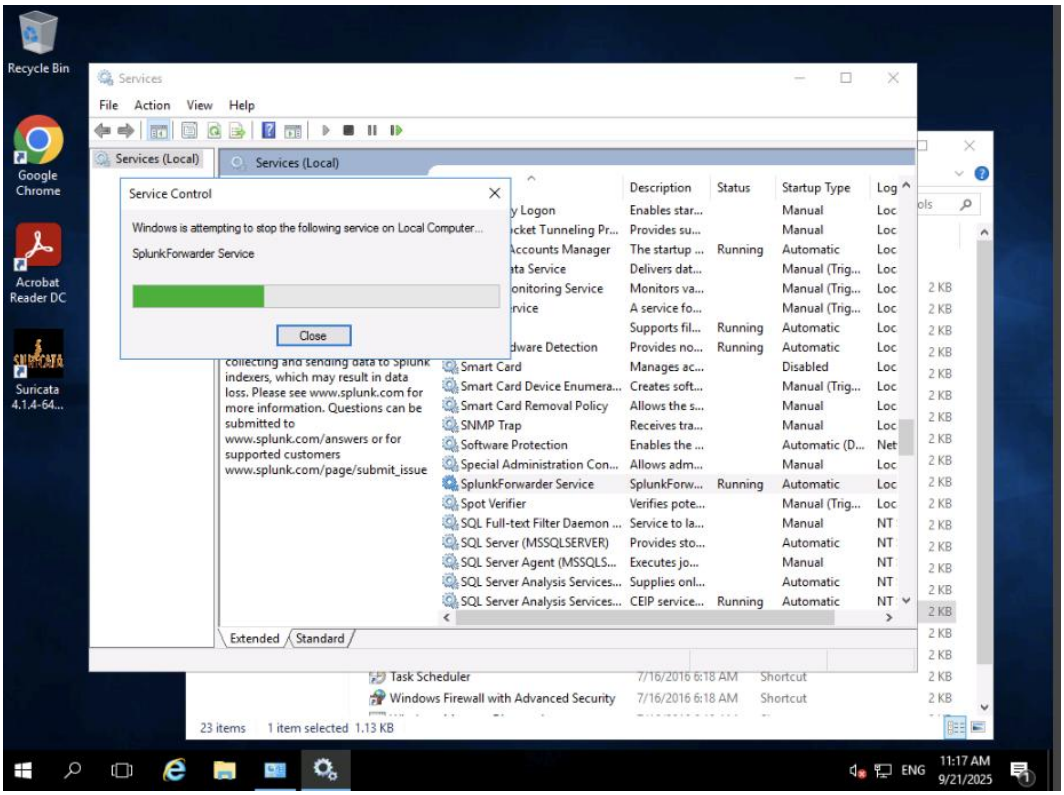

C:\Program Files\SplunkUniversalForwarder\etc\system\local\outputs.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts
suricata.yaml
inputs.conf
outputs.conf
[tcpout]
defaultGroup = default-autolb-group
[tcpout:default-autolb-group]
server = 10.10.1.2:9997
[tcpout-server://10.10.1.2:9997]
Normal text file
length : 143 lines : 9
Ln : 1 Col : 1 Sel : 0 | 0
Windows (CR LF)
UTF-8-BOM
INS
ENG
11:10 AM
9/21/2025

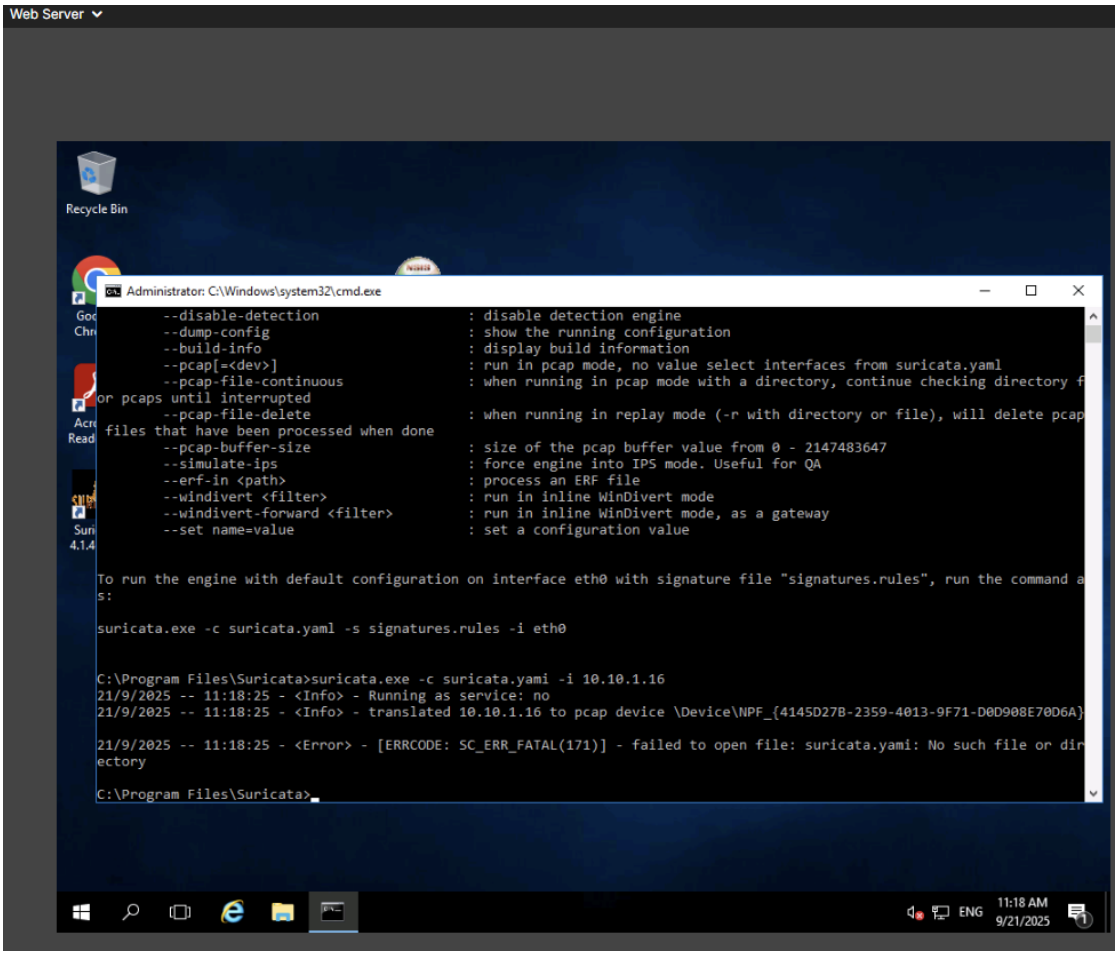

*C:\Program Files\SplunkUniversalForwarder\etc\system\local\outputs.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts
suricata.yaml
inputs.conf
outputs.conf
[tcpout]
defaultGroup = default-autolb-group
[tcpout:default-autolb-group]
server = 10.10.1.2:9997
[tcpout-server://10.10.1.2:9997]
[iis*]
Pulldown_type=true
MAXTIMESTAMPLOOKAHEAD =32
SHOULD_LINEMERGE = False
CHECK_FOR_HEADER
REPORT - iis2 =iis2
iis*
iis2

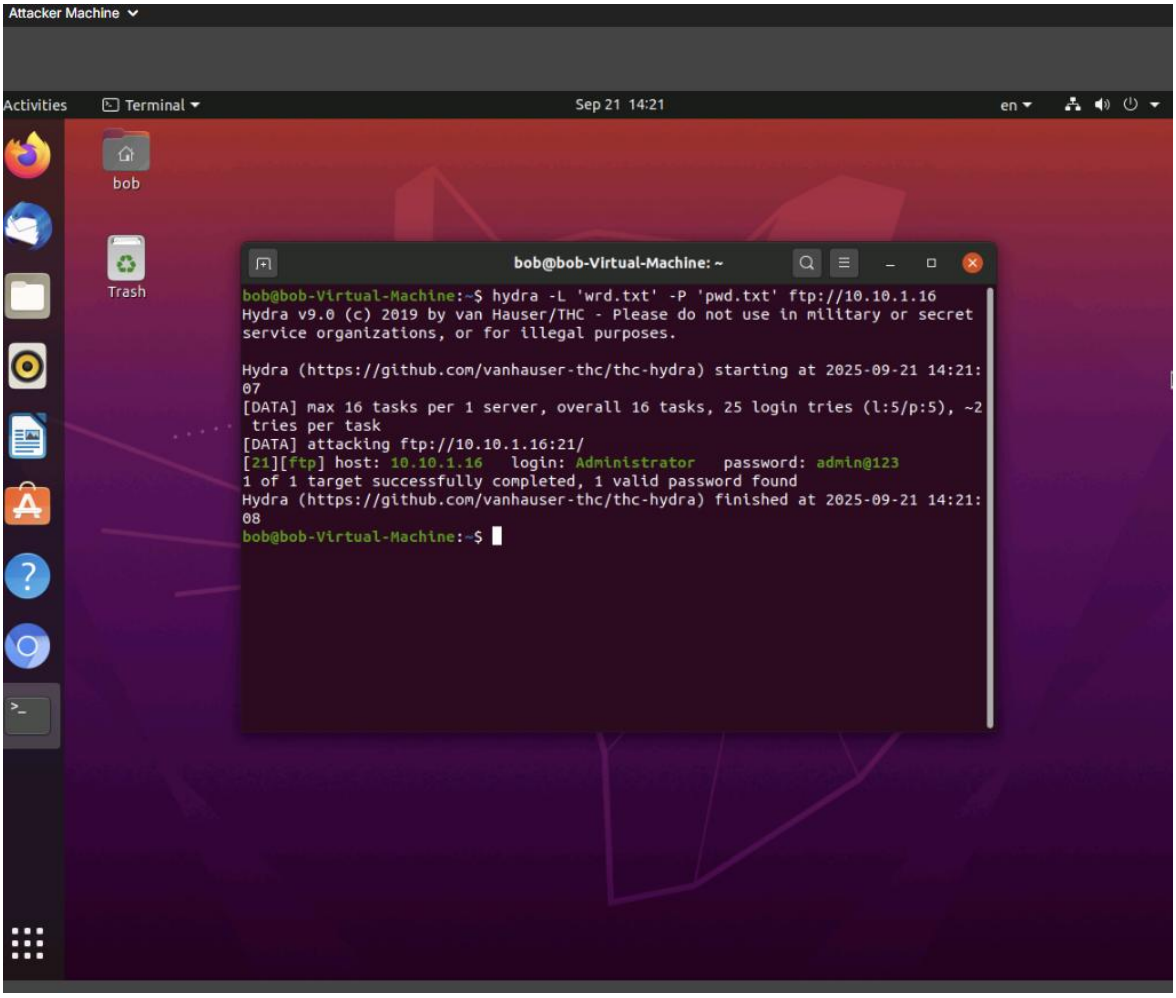

Untitled - Notepad
File Edit Format View Help
[iis*]
Pulldown_type=true
MAXTIMESTAMPLOOKAHEAD =32
SHOULD_LINEMERGE =False
CHECK_FOR_HEADER
REPORT -iis2 =iis2
5 items 1 item selected 264 bytes
ENG 11:11 AM 9/21/2025

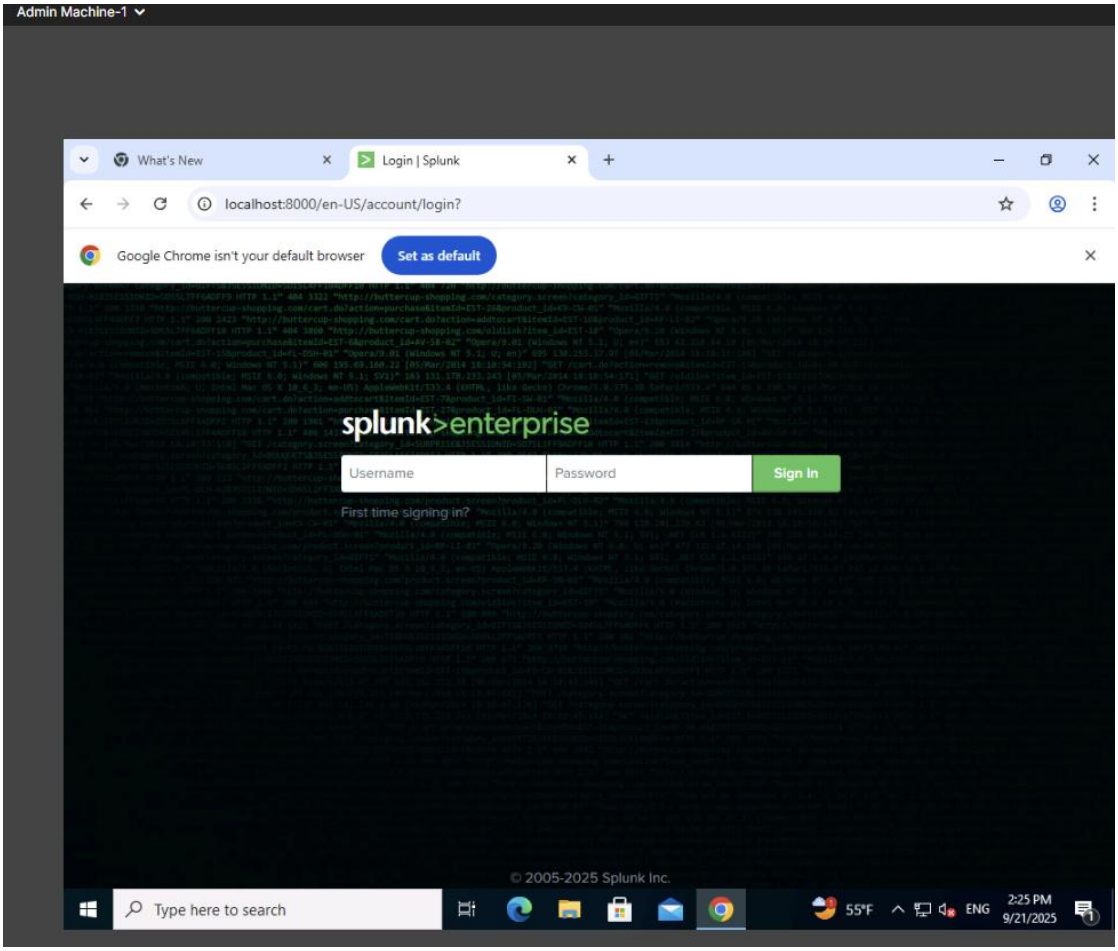

Untitled - Notepad
File Edit Format View Help
[default]
host -WebServer
[ignore_comments]
REGEX = ^#.*
DEST_KEY =queue
FORMAT =nullQueue
[iis2]
DELIMS =" "
FIELDS = date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User
6 items 1 item selected 264 bytes
ENG 11:13 AM 9/21/2025

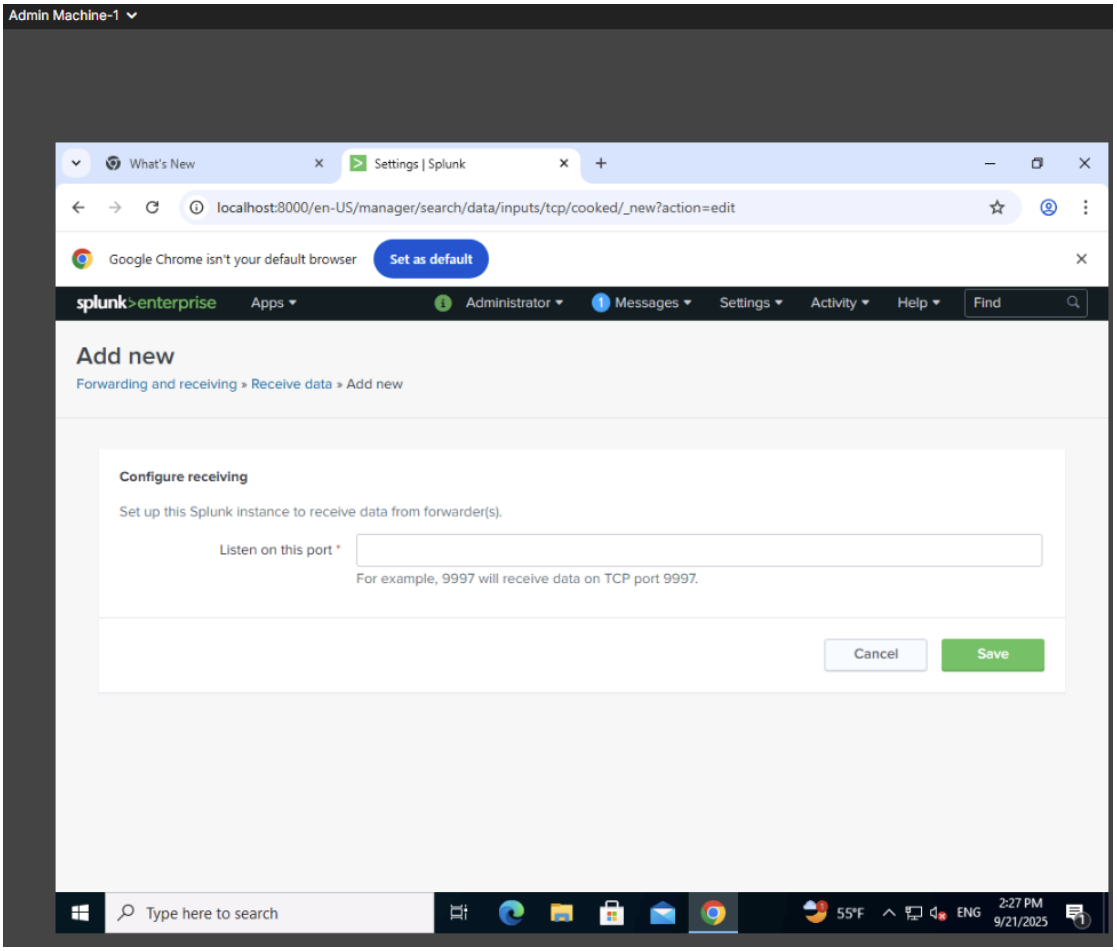

*C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts
suricata.yaml
inputs.conf
outputs.conf
1 [default]
2 [monitor://C:\inetpub\logs\logfiles]
3 sourcetype=iis
4 ignoreOlderThan =14d
5 host = WebServer
6
7 [monitor://C:\Program Files\Suricata\log]
8 sourcetyp=suricatata
9 ignoreOlderThan =14d
10 host = WebServer
Normal text file
length : 210 lines : 10
Ln : 6 Col : 1 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS
ENG
11:15 AM
9/21/2025

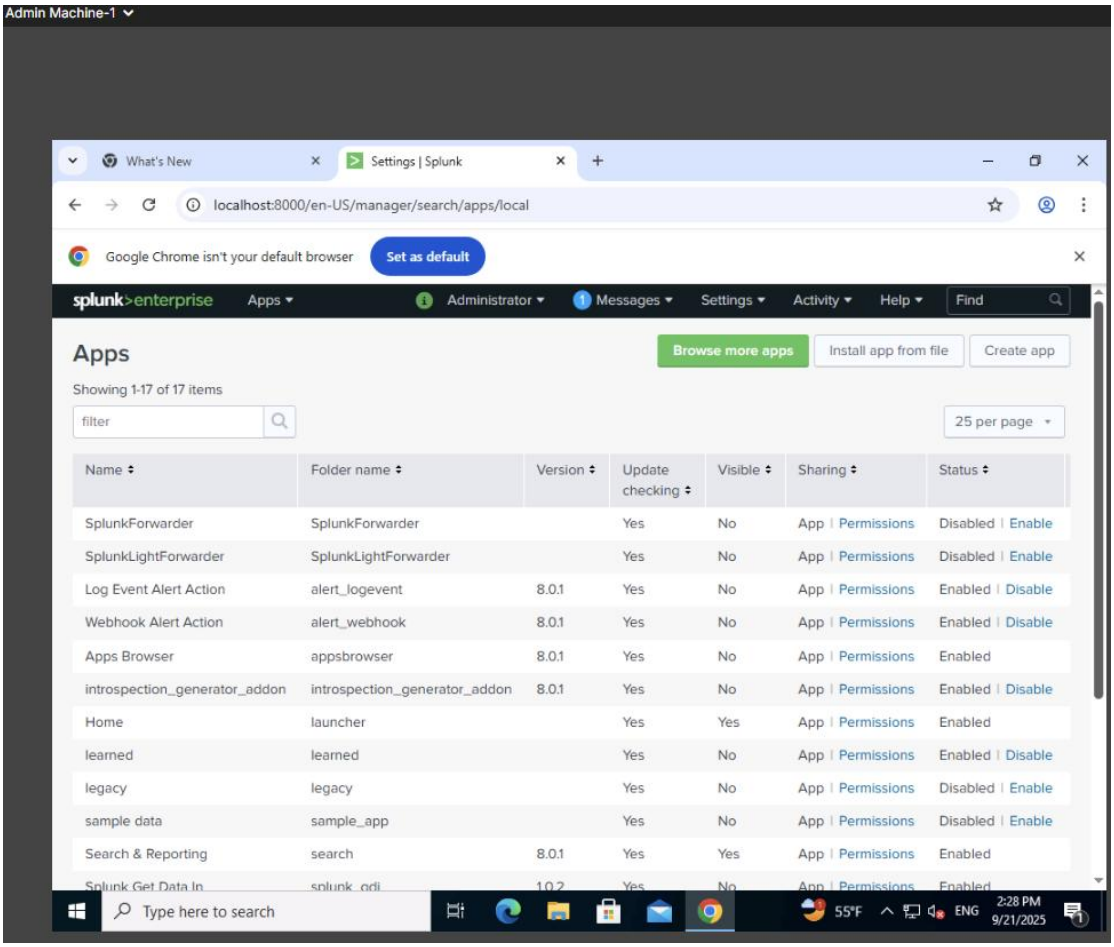

Recycle Bin
Google Chrome
Acrobat Reader DC
Suricata 4.1.4-64...
Services
File Action View Help
Services (Local)
Service Control
Windows is attempting to stop the following service on Local Computer...
SplunkForwarder Service
Close
collecting and sending data to Splunk indexers, which may result in data loss. Please see www.splunk.com for more information. Questions can be submitted to www.splunk.com/answers or for supported customers www.splunk.com/page/submit_issue
Description
Status
Startup Type
Smart Card
Smart Card Device Enumera...
Smart Card Removal Policy
SNMP Trap
Software Protection
Special Administration Con...
SplunkForwarder Service
Spot Verifier
SQL Full-text Filter Daemon ...
SQL Server (MSSQLSERVER)
SQL Server Agent (MSSQLS...
SQL Server Analysis Services...
SQL Server Analysis Services...
Extended
Standard
Task Scheduler
Windows Firewall with Advanced Security
23 items
1 item selected 1.13 KB
ENG
11:17 AM
9/21/2025

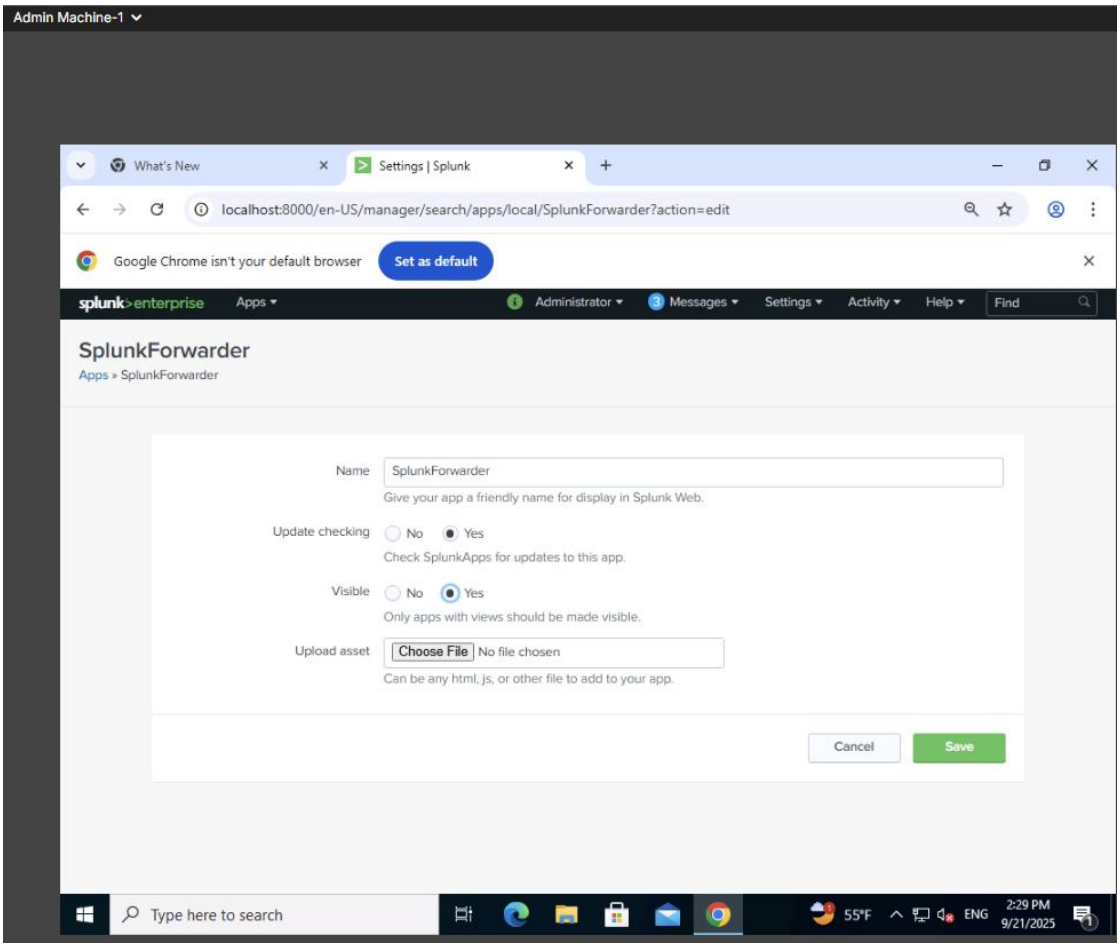

Web Server
Recycle Bin
Administrator: C:\Windows\system32\cmd.exe
--disable-detection : disable detection engine
--dump-config : show the running configuration
--build-info : display build information
--pcap[=<dev>] : run in pcap mode, no value select interfaces from suricata.yaml
--pcap-file-continuous : when running in pcap mode with a directory, continue checking directory f
or pcaps until interrupted
--pcap-file-delete : when running in replay mode (-r with directory or file), will delete pcap
files that have been processed when done
--pcap-buffer-size : size of the pcap buffer value from 0 - 2147483647
--simulate-ips : force engine into IPS mode. Useful for QA
--erf-in <path> : process an ERF file
--windivert <filter> : run in inline WinDivert mode
--windivert-forward <filter> : run in inline WinDivert mode, as a gateway
--set name=value : set a configuration value
To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the command a
s:
suricata.exe -c suricata.yaml -s signatures.rules -i eth0
C:\Program Files\Suricata>suricata.exe -c suricata.yami -i 10.10.1.16
21/9/2025 -- 11:18:25 - <Info> - Running as service: no
21/9/2025 -- 11:18:25 - <Info> - translated 10.10.1.16 to pcap device \Device\NPF_{4145D27B-2359-4013-9F71-D0D908E70D6A}
21/9/2025 -- 11:18:25 - <Error> - [ERRCODE: SC_ERR_FATAL(171)] - failed to open file: suricata.yami: No such file or dir
ectory
C:\Program Files\Suricata>
ENG
11:18 AM
9/21/2025

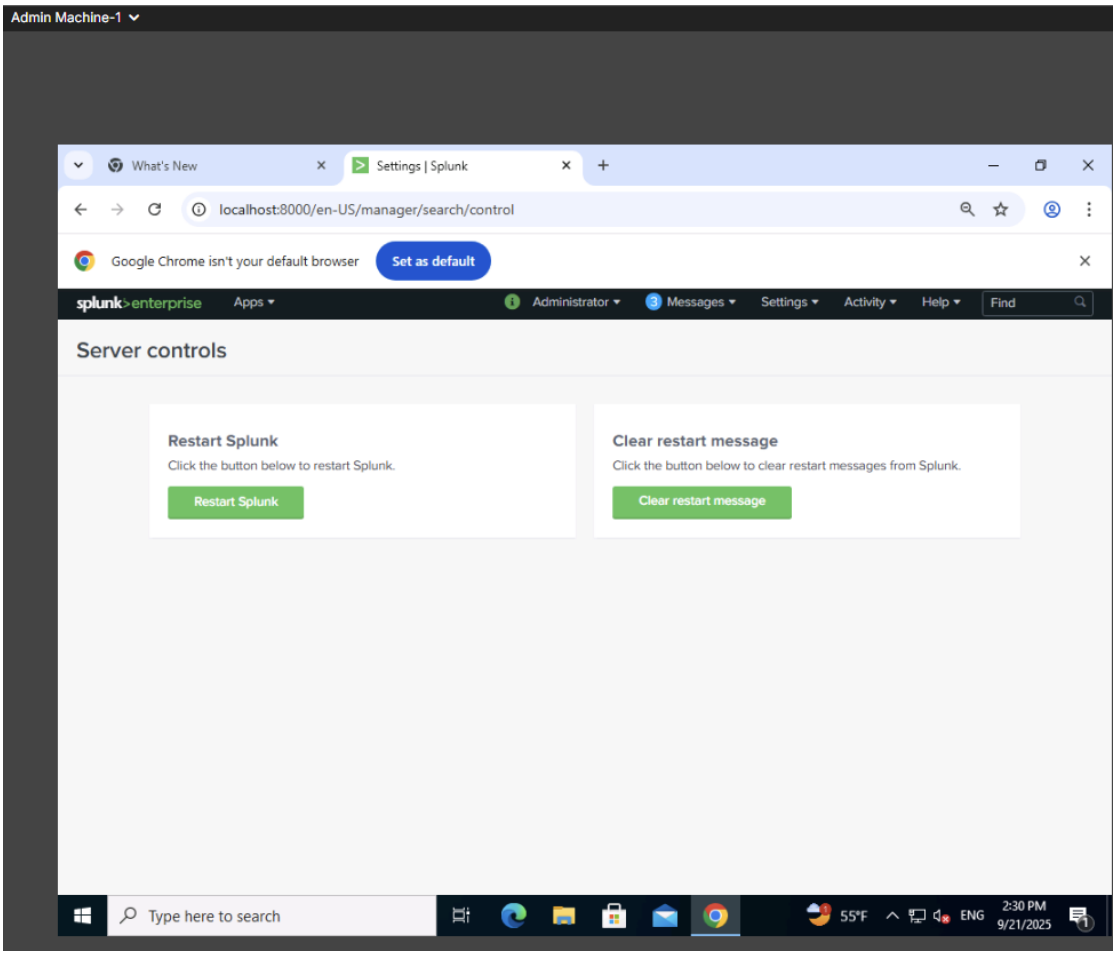

Attacker Machine
Activities
Terminal
Sep 21 14:21
en
bob
Trash
bob@bob-Virtual-Machine: ~
bob@bob-Virtual-Machine:~$ hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-21 14:21:07
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ftp://10.10.1.16:21/
[21][ftp] host: 10.10.1.16 login: Administrator password: admin@123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-21 14:21:08
bob@bob-Virtual-Machine:~$

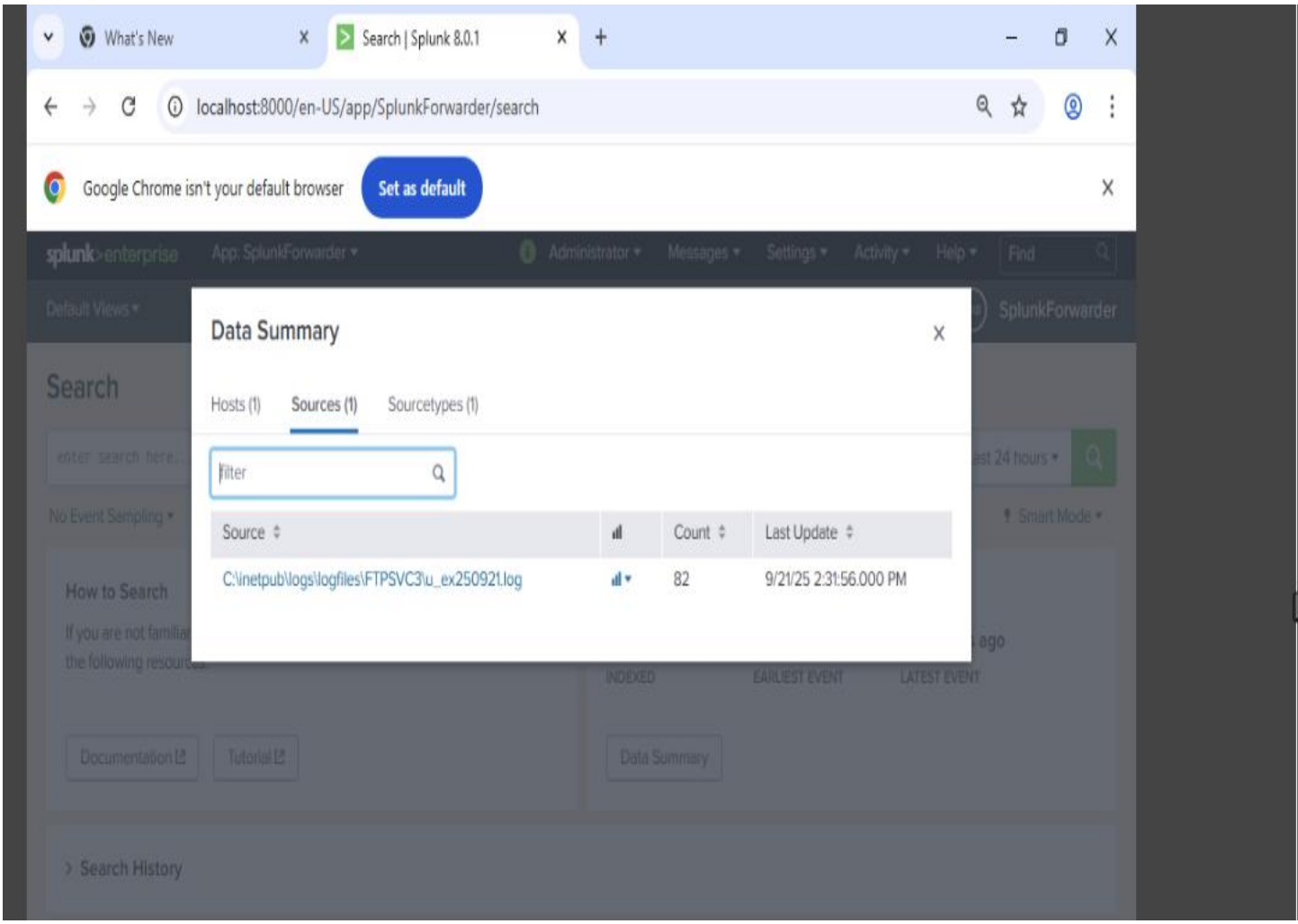

Admin Machine-1
What's New
Login | Splunk
localhost:8000/en-US/account/login?
Google Chrome isn't your default browser
Set as default
splunk>enterprise
Username
Password
Sign In
First time signing in?
© 2005-2025 Splunk Inc.
Type here to search
55°F
ENG
2:25 PM
9/21/2025

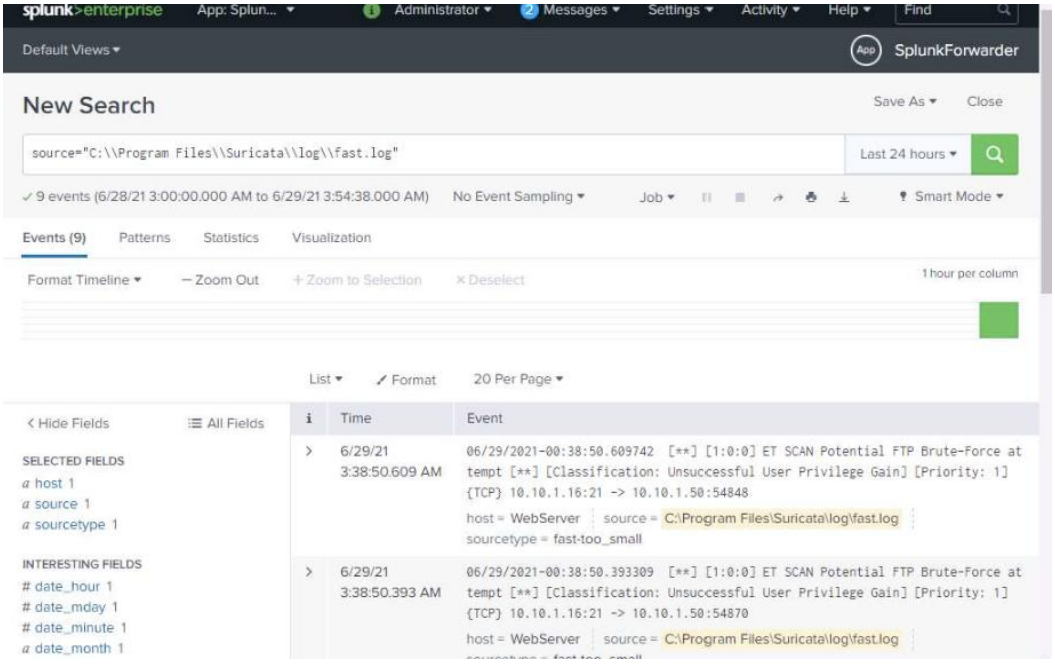

Admin Machine-1
What's New
Settings | Splunk
localhost:8000/en-US/manager/search/data/inputs/tcp/cooked/_new?action=edit
Google Chrome isn't your default browser
Set as default
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add new
Forwarding and receiving » Receive data » Add new
Configure receiving
Set up this Splunk instance to receive data from forwarder(s).
Listen on this port *
For example, 9997 will receive data on TCP port 9997.
Cancel
Save
Type here to search
55°F
ENG
2:27 PM
9/21/2025

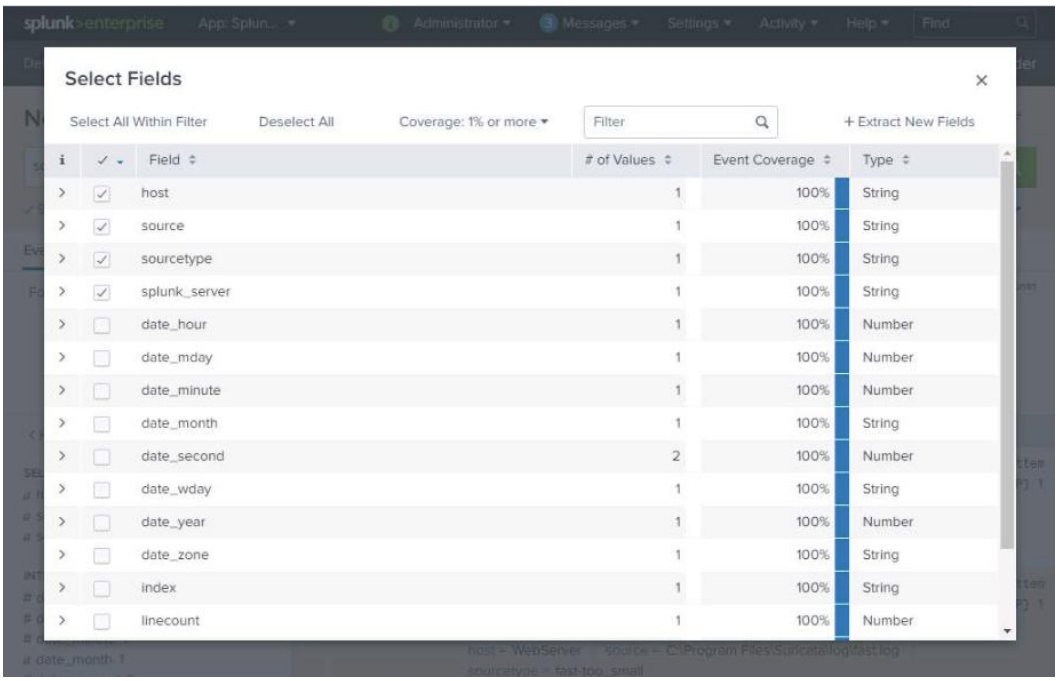

Admin Machine-1
What's New
Settings | Splunk
localhost:8000/en-US/manager/search/apps/local
Google Chrome isn't your default browser
Set as default
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Browse more apps
Install app from file
Create app
Showing 1-17 of 17 items
filter
25 per page
Name
Folder name
Version
Update checking
Visible
Sharing
Status
SplunkForwarder SplunkForwarder Yes No App | Permissions Disabled | Enable
SplunkLightForwarder SplunkLightForwarder Yes No App | Permissions Disabled | Enable
Log Event Alert Action alert_logevent 8.0.1 Yes No App | Permissions Enabled | Disable
Webhook Alert Action alert_webhook 8.0.1 Yes No App | Permissions Enabled | Disable
Apps Browser appsbrowser 8.0.1 Yes No App | Permissions Enabled
introspection_generator_addon introspection_generator_addon 8.0.1 Yes No App | Permissions Enabled | Disable
Home launcher Yes Yes App | Permissions Enabled
learned learned Yes No App | Permissions Enabled | Disable
legacy legacy Yes No App | Permissions Disabled | Enable
sample data sample_app Yes No App | Permissions Disabled | Enable
Search & Reporting search 8.0.1 Yes Yes App | Permissions Enabled
Type here to search
55°F
ENG
2:28 PM
9/21/2025

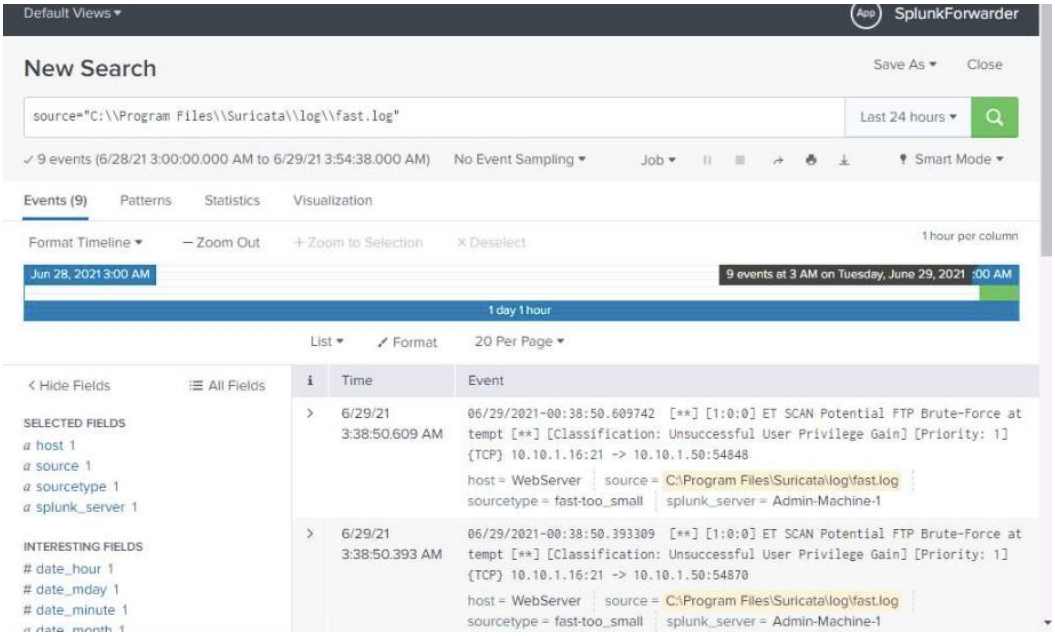

Admin Machine-1
What's New
Settings | Splunk
localhost:8000/en-US/manager/search/apps/local/SplunkForwarder?action=edit
Google Chrome isn't your default browser
Set as default
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
SplunkForwarder
Apps » SplunkForwarder
Name
SplunkForwarder
Give your app a friendly name for display in Splunk Web.
Update checking
No
Yes
Check SplunkApps for updates to this app.
Visible
No
Yes
Only apps with views should be made visible.
Upload asset
Choose File
No file chosen
Can be any html, js, or other file to add to your app.
Cancel
Save
Type here to search
55°F
ENG
2:29 PM
9/21/2025


Admin Machine-1
What's New
Settings | Splunk
localhost:8000/en-US/manager/search/control
Google Chrome isn't your default browser
Set as default
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Server controls
Restart Splunk
Click the button below to restart Splunk.
Restart Splunk
Clear restart message
Click the button below to clear restart messages from Splunk.
Clear restart message
Type here to search
55°F
ENG
2:30 PM
9/21/2025


What's New
Search | Splunk 8.0.1
localhost:8000/en-US/app/SplunkForwarder/search
Google Chrome isn't your default browser
Set as default
splunk>enterprise
App: SplunkForwarder
Administrator
Messages
Settings
Activity
Help
Find
Default Views
SplunkForwarder
Search
Data Summary
Hosts (1)
Sources (1)
Sourcetypes (1)
filter
Source
Count
Last Update
C:\inetpub\logs\logfiles\FTPSVC3\u_ex250921.log
82
9/21/25 2:31:56.000 PM
How to Search
Documentation
Tutorial
Data Summary
Search History


splunk>enterprise
App: Splun...
Administrator
Messages
Settings
Activity
Help
Find
Default Views
SplunkForwarder
New Search
Save As
Close
source="C:\\Program Files\\Suricata\\log\\fast.log"
Last 24 hours
9 events (6/28/21 3:00:00.000 AM to 6/29/21 3:54:38.000 AM)
No Event Sampling
Job
Smart Mode
Events (9)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 1
a date_month 1
Time
Event
6/29/21 3:38:50.609 AM
06/29/2021-00:38:50.609742 [**] [1:0:0] ET SCAN Potential FTP Brute-Force attempt [**] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:54848
host = WebServer source = C:\Program Files\Suricata\log\fast.log
sourcetype = fast-too_small
6/29/21 3:38:50.393 AM
06/29/2021-00:38:50.393309 [**] [1:0:0] ET SCAN Potential FTP Brute-Force attempt [**] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:54870
host = WebServer source = C:\Program Files\Suricata\log\fast.log





Exercise 7: Detect Malicious Network Traffic using HoneyBOT

Lab Scenario

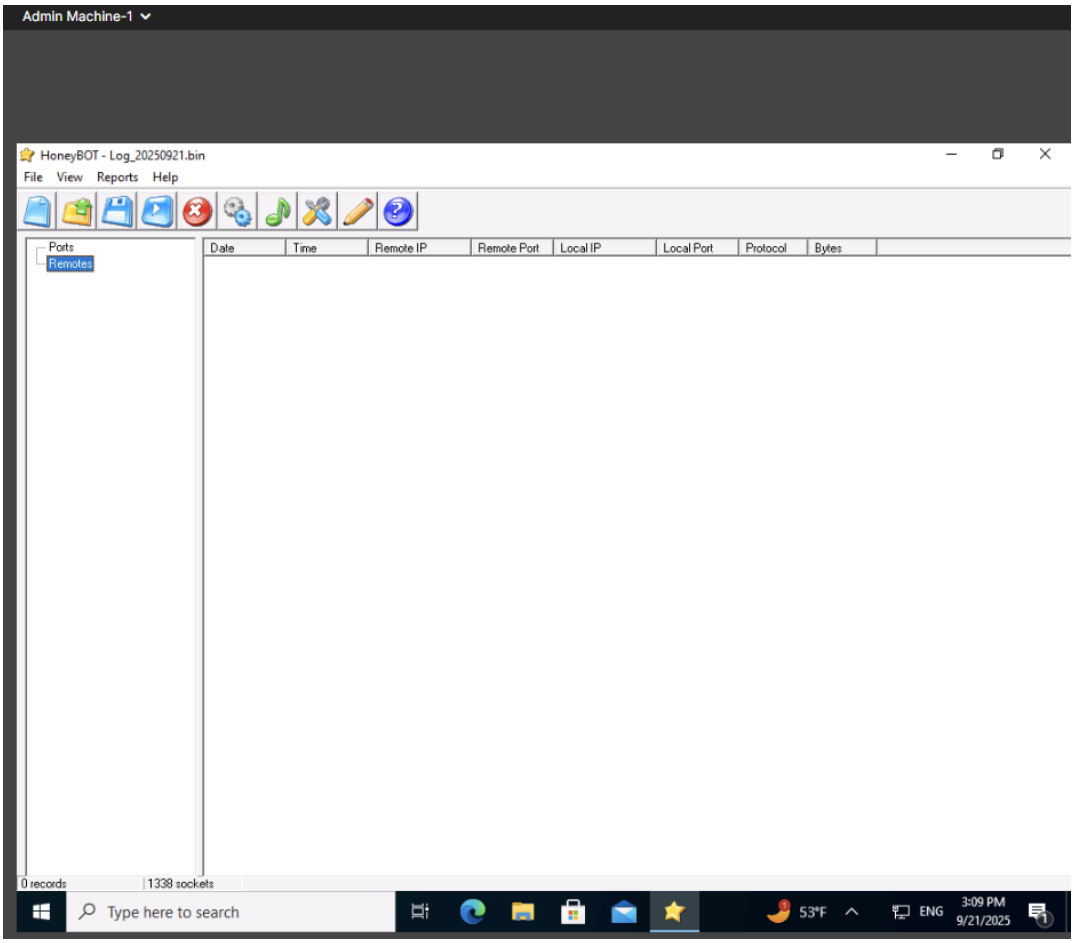
Network traffic is the amount of data packets passing through a network.

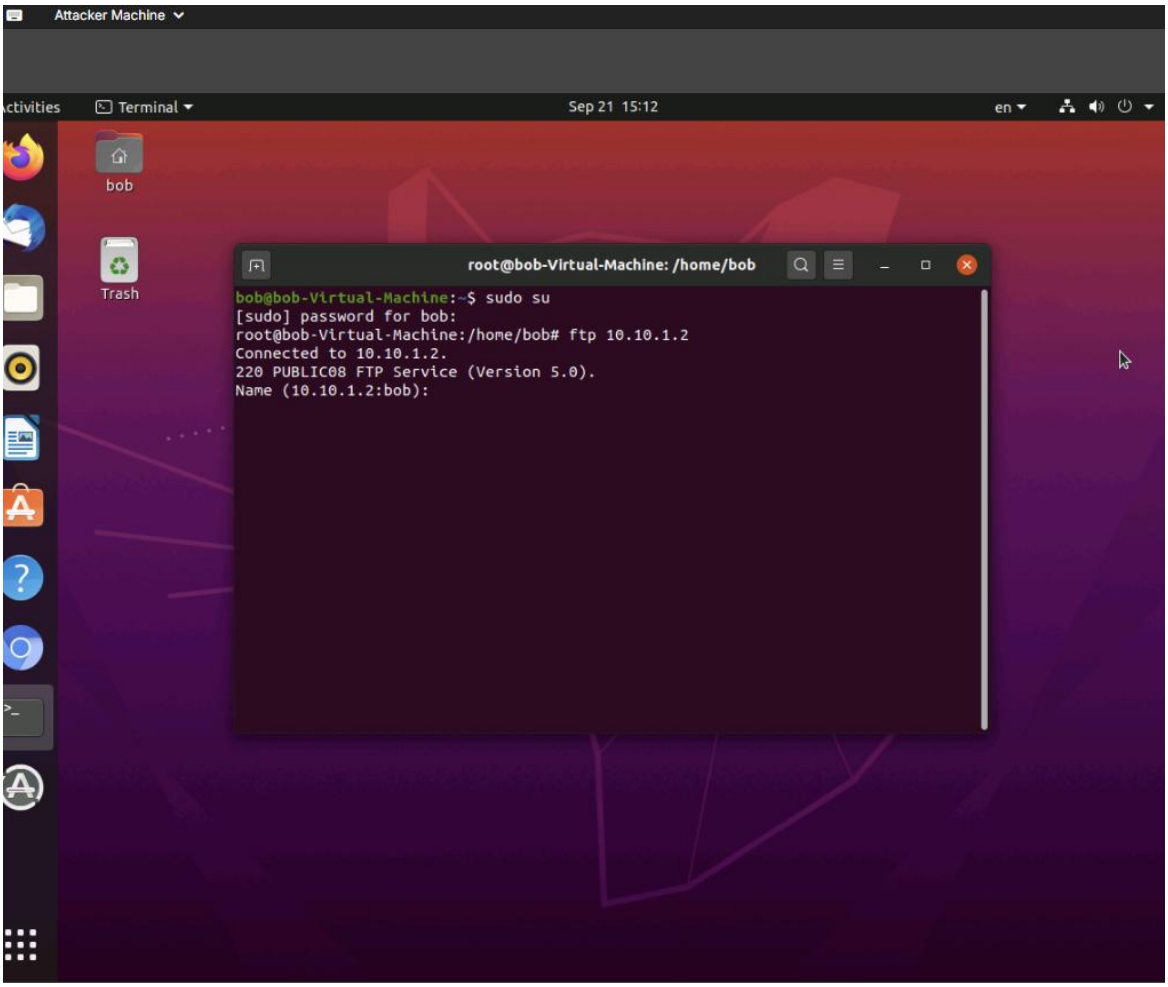
Lab Objectives

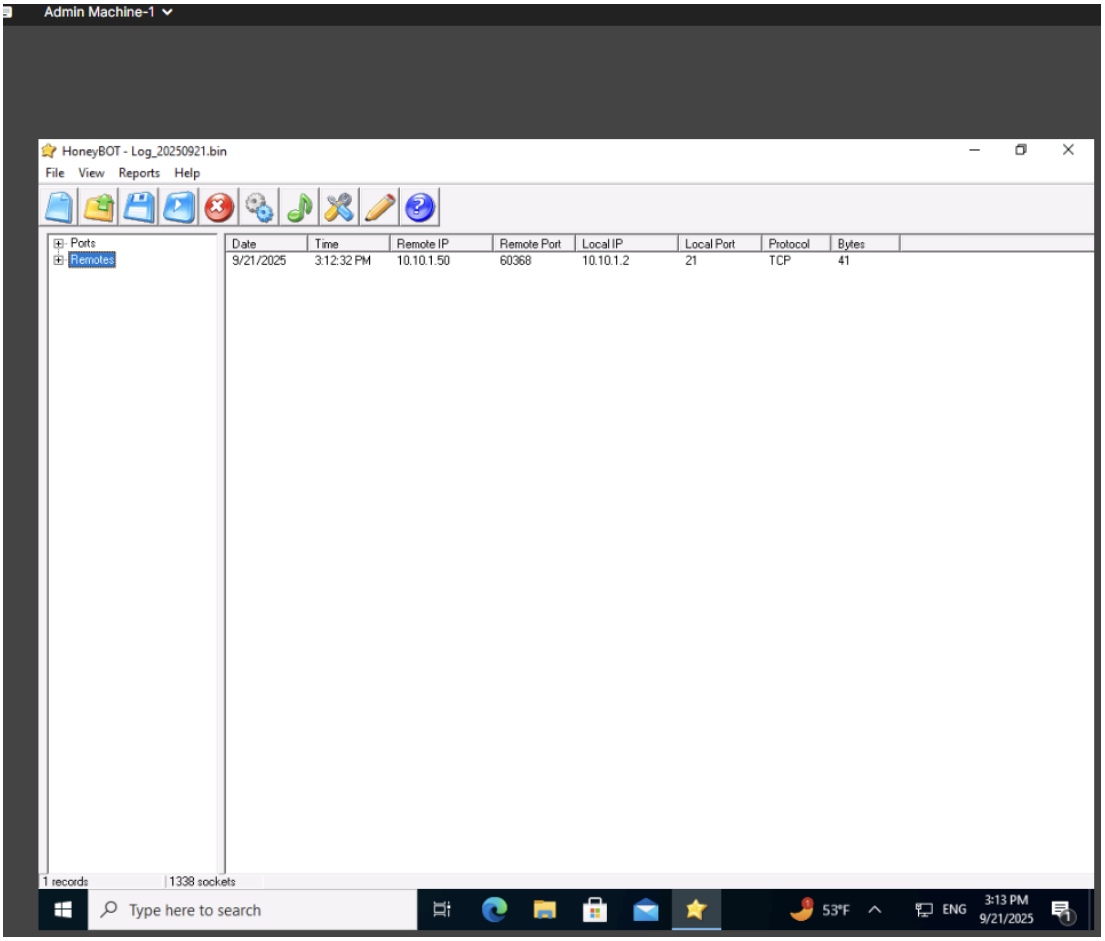
This lab demonstrates how to detect malicious network traffic using HoneyBot.

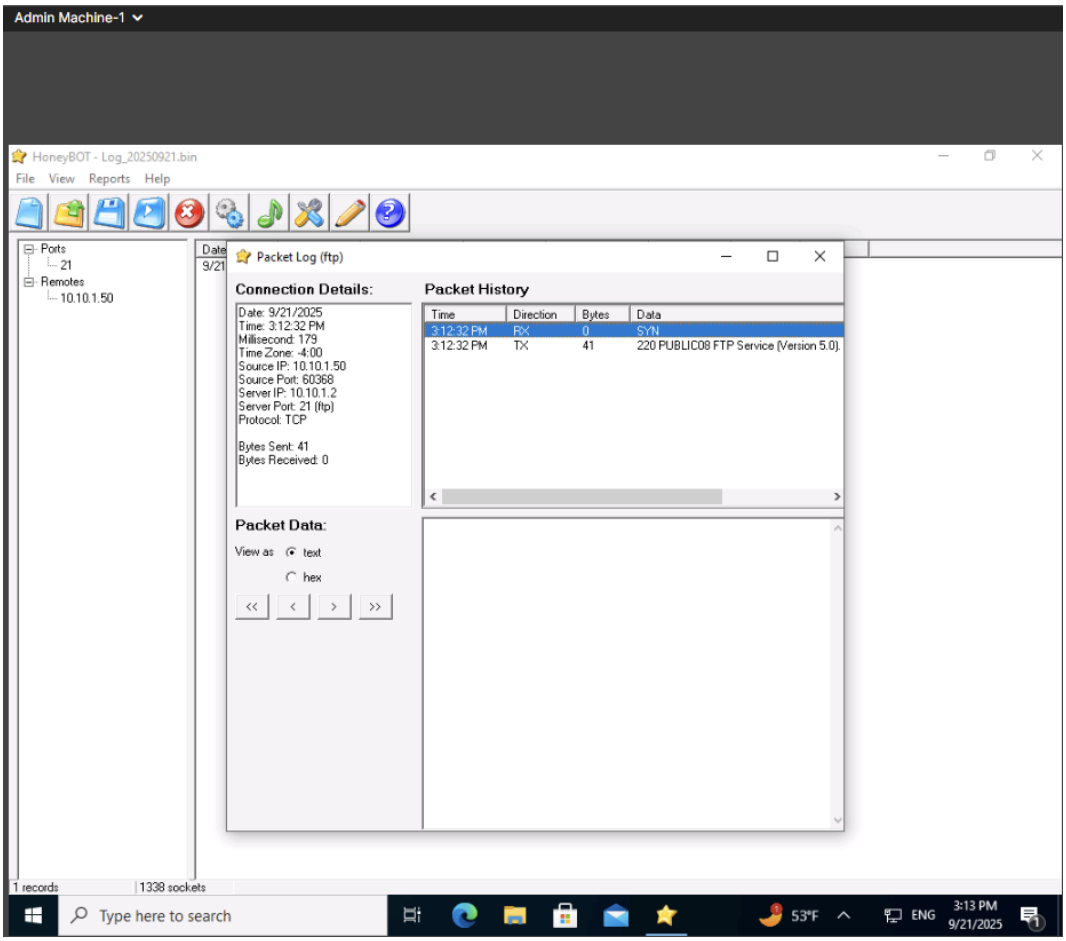
Overview of Network Traffic

Normal traffic behavior is based on various behavioral attributes such as normal email activity, reasonable number of failed attempts and normal processor usage. Any activity that does not match normal behavior can be treated as an attack.




Attacker Machine
Activities
Terminal
Sep 21 15:12
en
bob
Trash
root@bob-Virtual-Machine: /home/bob
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# ftp 10.10.1.2
Connected to 10.10.1.2.
220 PUBLIC08 FTP Service (Version 5.0).
Name (10.10.1.2:bob):


Admin Machine-1
HoneyBOT - Log_20250921.bin
File View Reports Help
Ports
Remotes
Date Time Remote IP Remote Port Local IP Local Port Protocol Bytes
9/21/2025 3:12:32 PM 10.10.1.50 60368 10.10.1.2 21 TCP 41
1 records
1338 sockets
Type here to search
53°F
ENG
3:13 PM
9/21/2025



Exercise 8: Establishing Virtual Private Network Connection using SoftEther VPN

SoftEther VPN Server, Client, and Bridge are free and open-source software. SoftEther VPN is a strong tool that can be used to build a VPN tunnel.

Lab Scenario

In an organization's network infrastructure, there are firewalls to isolate internal and external network traffic to ensure security. Organizations use firewalls, proxies, and Network Address Translators (NATs) not only to resolve security issues but also to share IP addresses with users in the office. These devices play a crucial role nowadays.

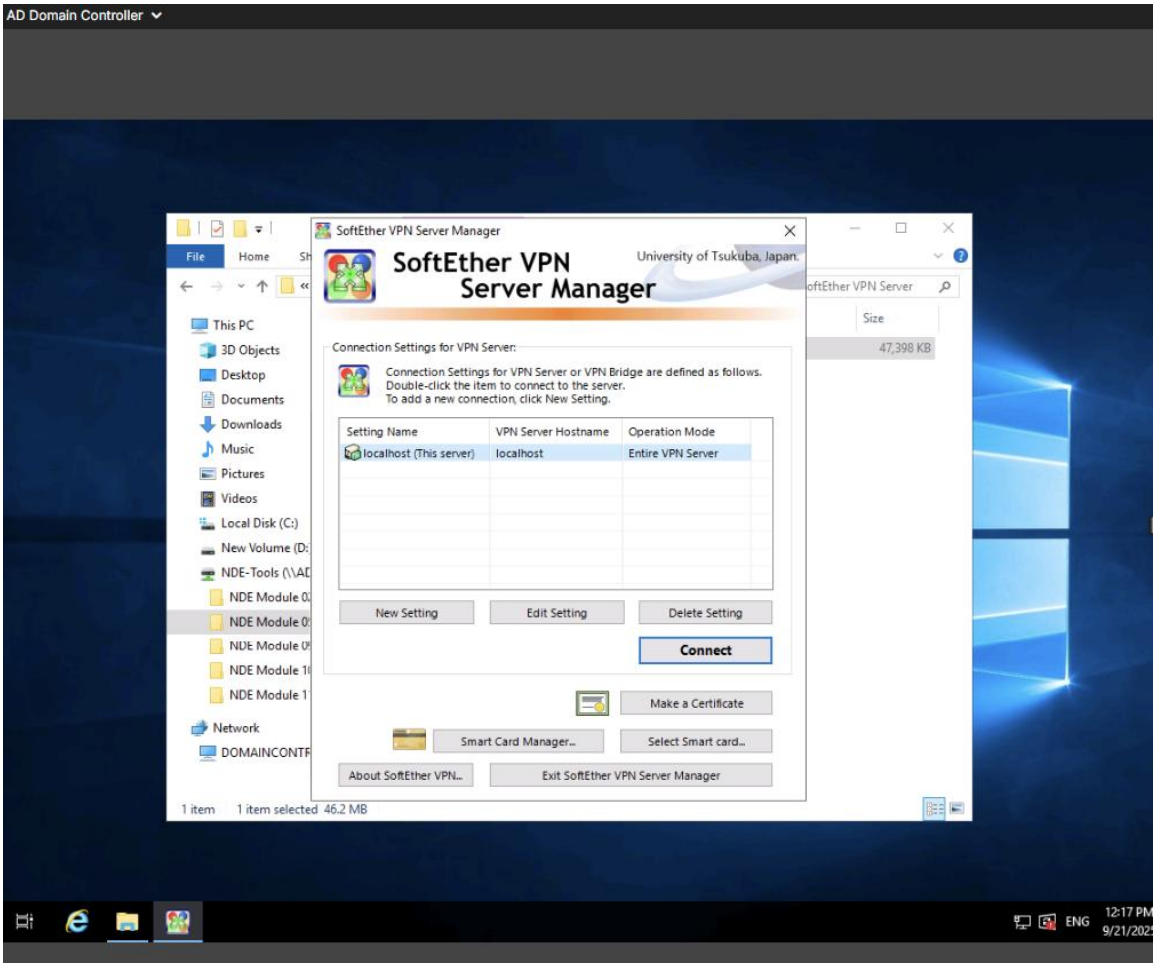
Lab Objectives

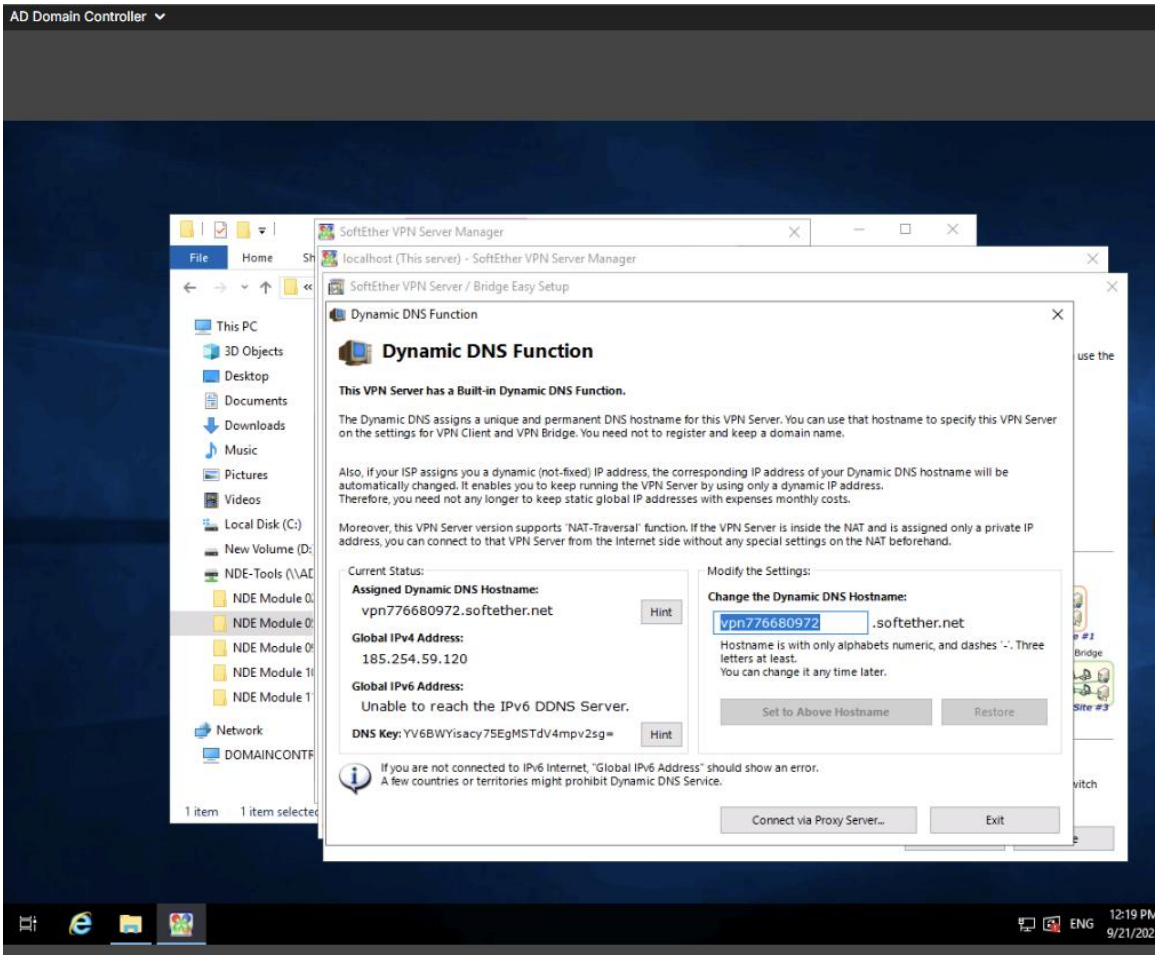
This lab will demonstrate how to establish a Virtual Private Network (VPN) connection using SoftEther VPN.

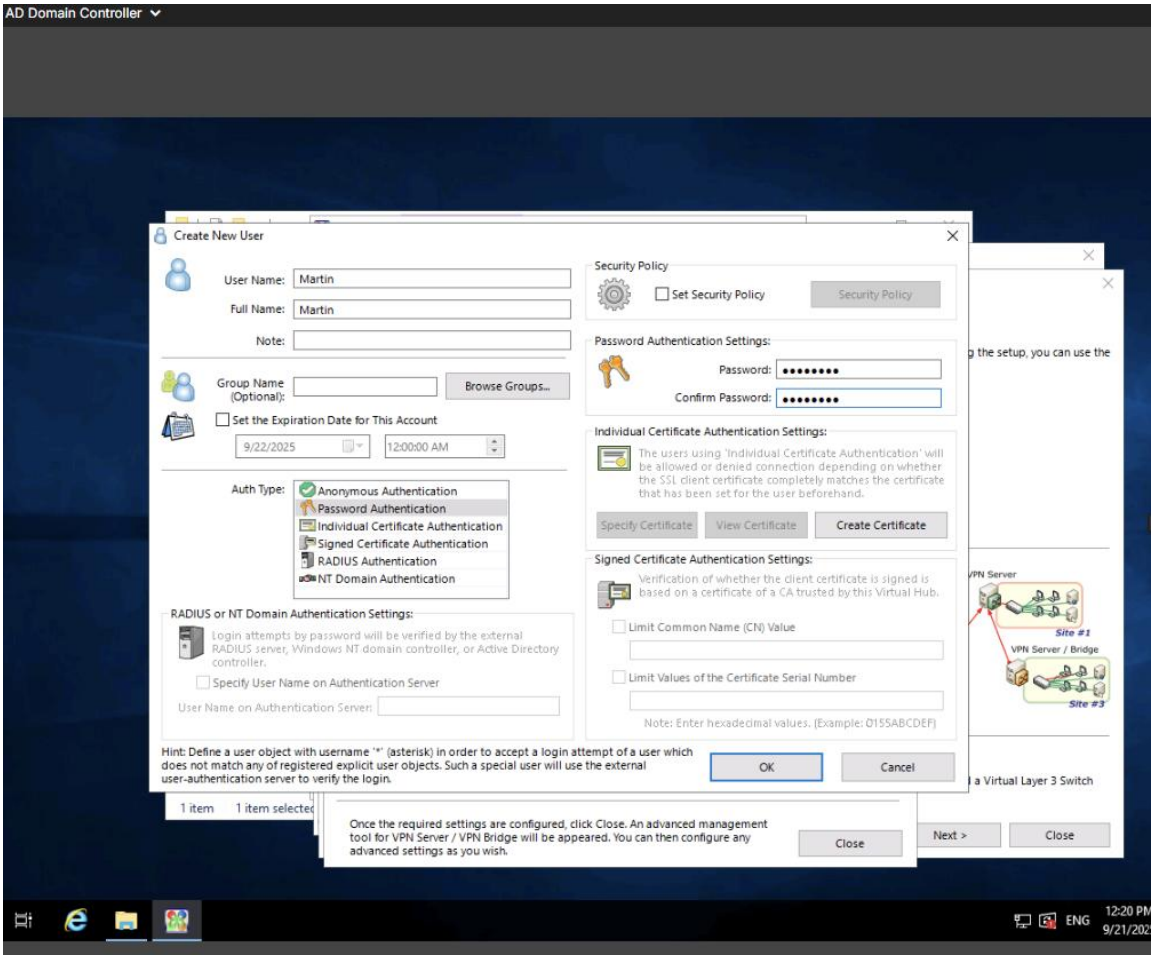
Overview of SoftEther VPN

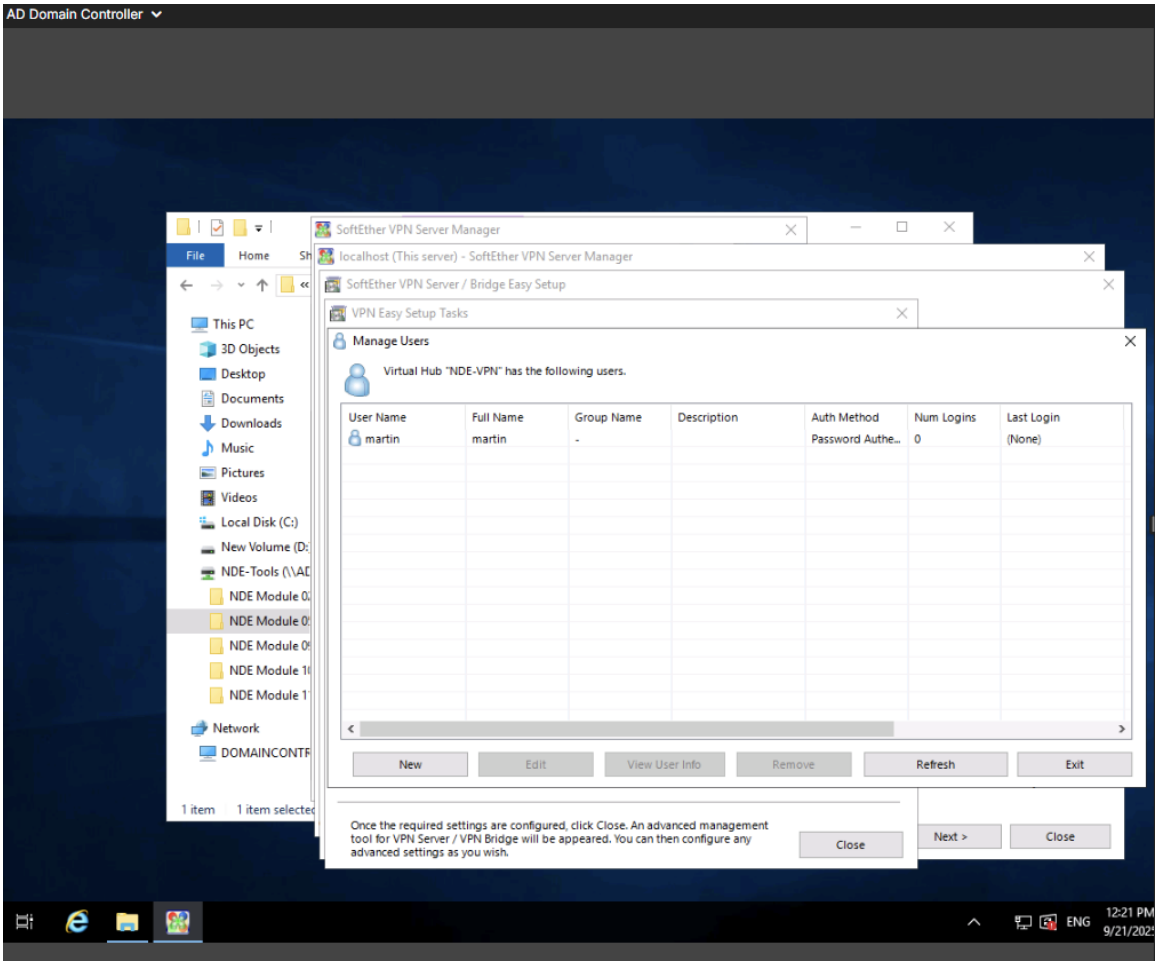
SoftEther VPN is one of the most powerful and easy-to-use VPN software worldwide. SoftEther VPN is freeware. One of the key features of SoftEther VPN is the transparency for firewalls, proxy servers, and NATs. NATs are sometimes implemented on broadband router products.

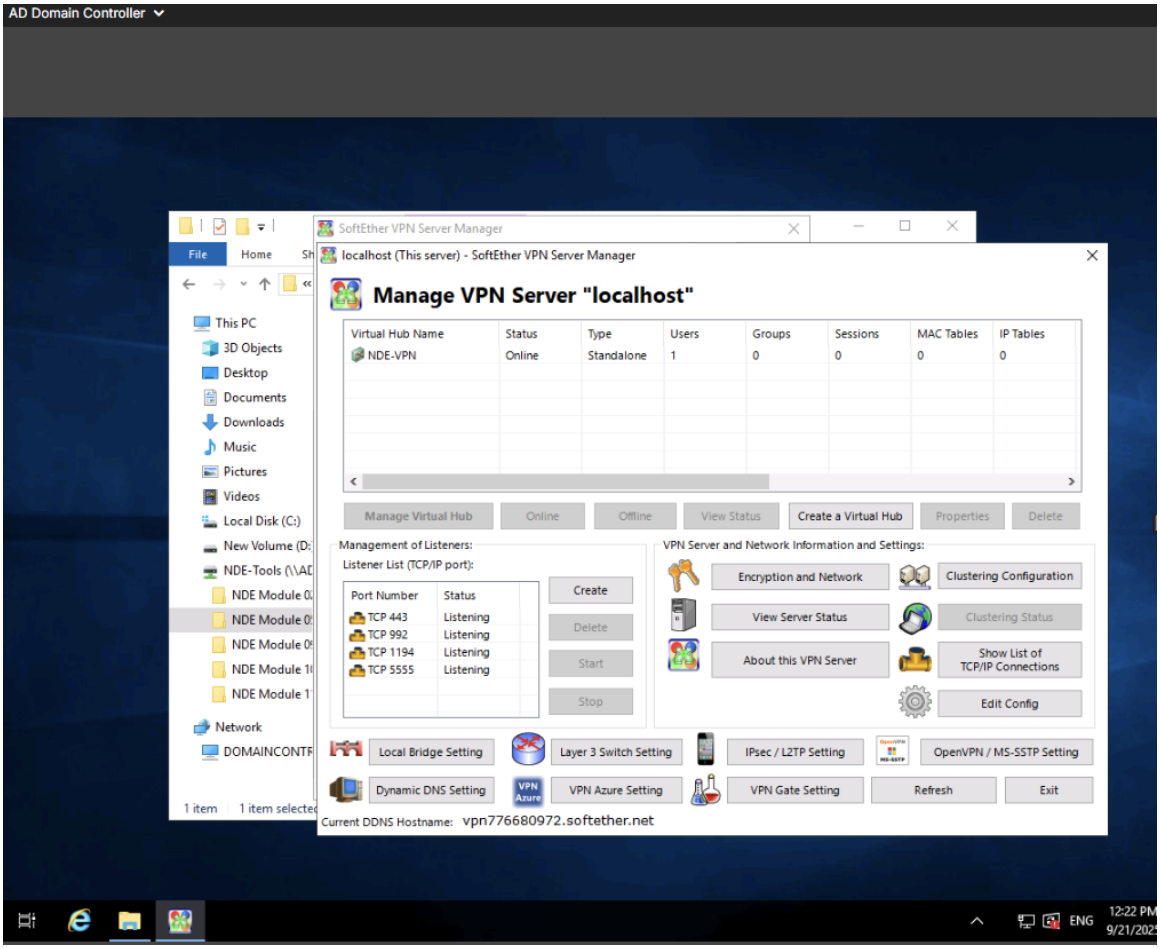
SoftEther VPN uses HTTPS protocol in order to establish a VPN tunnel. HTTPS (HTTP over SSL) protocol uses the 443 of TCP/IP port as destination. This port is well-known, and almost all firewalls, proxy servers, and NATs can pass packets using the HTTPS protocol.

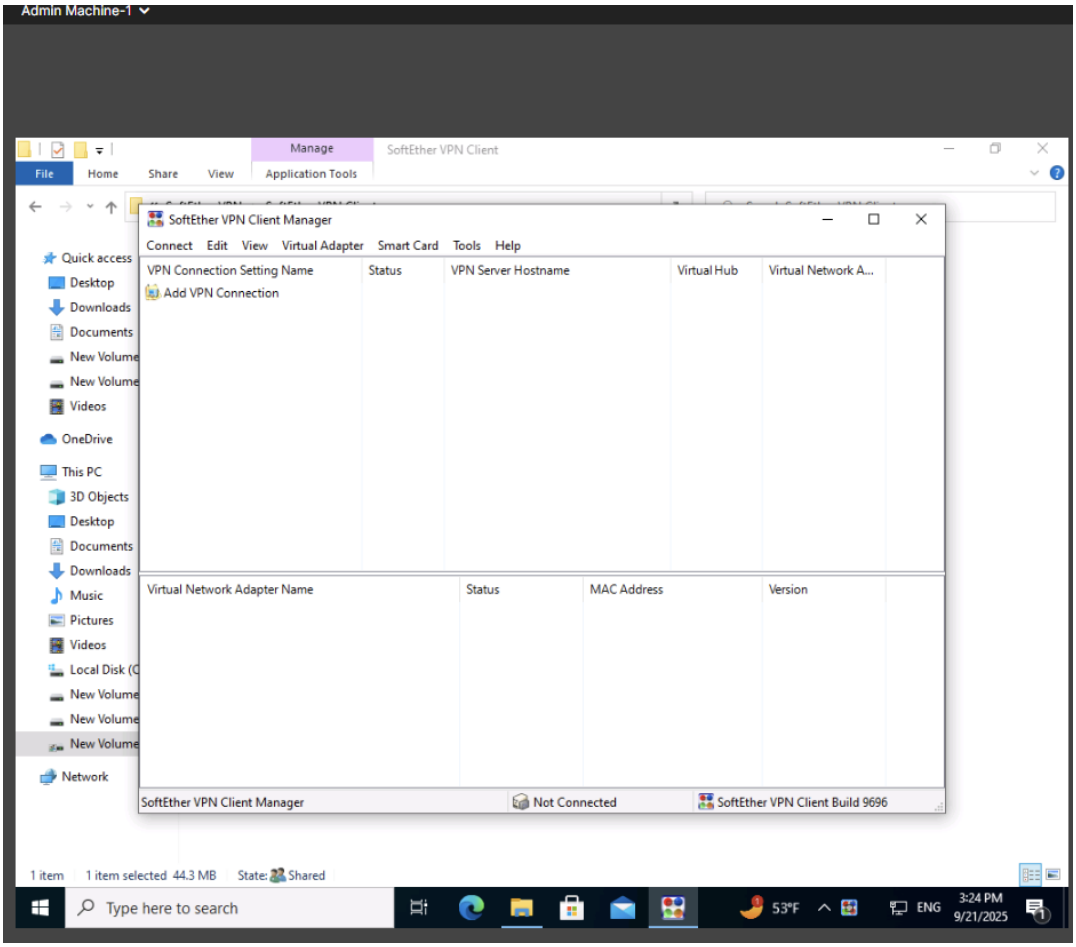


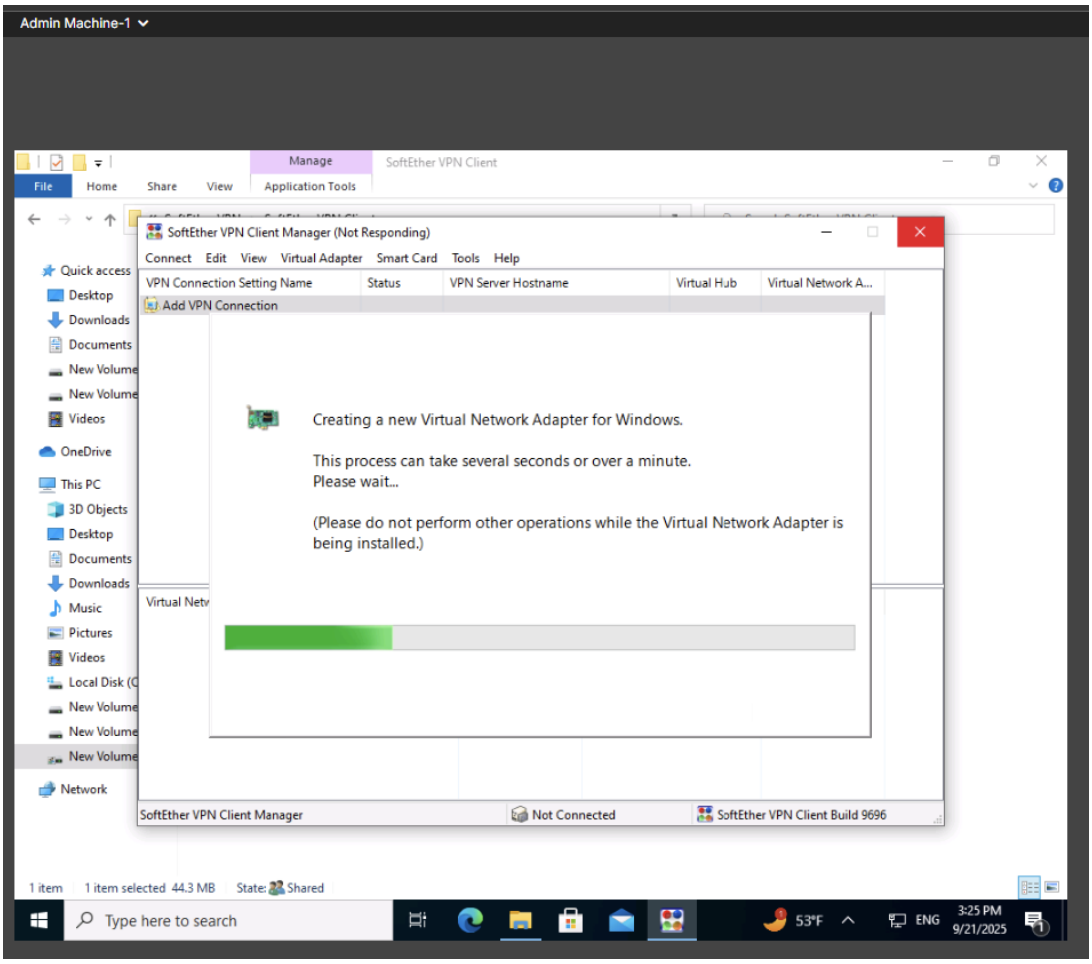

AD Domain Controller
SoftEther VPN Server Manager
localhost (This server) - SoftEther VPN Server Manager
SoftEther VPN Server / Bridge Easy Setup
Dynamic DNS Function
Dynamic DNS Function
This VPN Server has a Built-in Dynamic DNS Function.
The Dynamic DNS assigns a unique and permanent DNS hostname for this VPN Server. You can use that hostname to specify this VPN Server on the settings for VPN Client and VPN Bridge. You need not to register and keep a domain name.
Also, if your ISP assigns you a dynamic (not-fixed) IP address, the corresponding IP address of your Dynamic DNS hostname will be automatically changed. It enables you to keep running the VPN Server by using only a dynamic IP address.
Therefore, you need not any longer to keep static global IP addresses with expenses monthly costs.
Moreover, this VPN Server version supports 'NAT-Traversal' function. If the VPN Server is inside the NAT and is assigned only a private IP address, you can connect to that VPN Server from the Internet side without any special settings on the NAT beforehand.
Current Status:
Assigned Dynamic DNS Hostname:
vpn776680972.softether.net
Hint
Global IPv4 Address:
185.254.59.120
Global IPv6 Address:
Unable to reach the IPv6 DDNS Server.
DNS Key: YV6BWYisacy75EgMSTdV4mpv2sg=
Hint
Modify the Settings:
Change the Dynamic DNS Hostname:
vpn776680972
.softether.net
Hostname is with only alphabets numeric, and dashes '-'. Three letters at least.
You can change it any time later.
Set to Above Hostname
Restore
If you are not connected to IPv6 Internet, "Global IPv6 Address" should show an error.
A few countries or territories might prohibit Dynamic DNS Service.
Connect via Proxy Server...
Exit
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:
NDE-Tools (\\AD
NDE Module 0
NDE Module 0
NDE Module 0
NDE Module 1
NDE Module 1
Network
DOMAINCONTR
1 item
1 item selected
ENG
12:19 PM
9/21/202

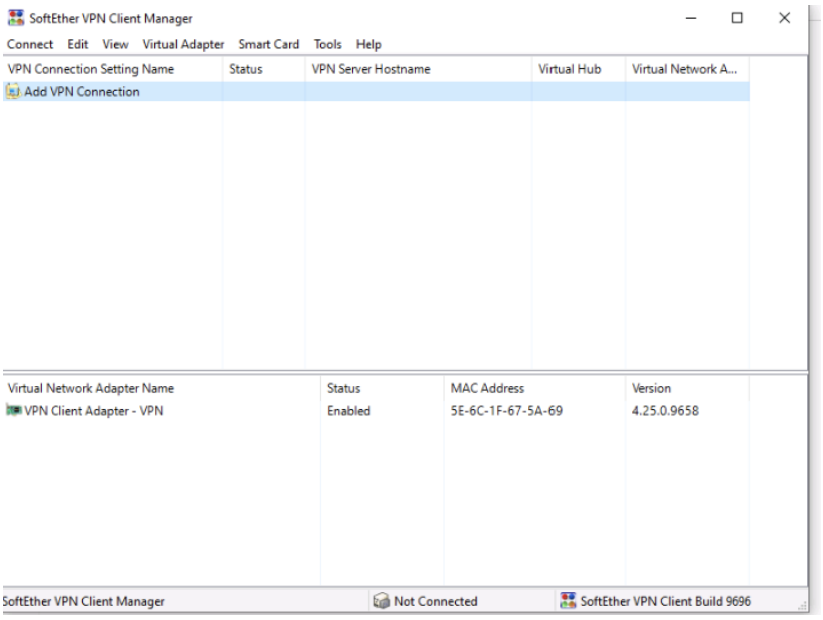

AD Domain Controller
Create New User
User Name: Martin
Full Name: Martin
Note:
Group Name (Optional):
Browse Groups...
Set the Expiration Date for This Account
9/22/2025
12:00:00 AM
Auth Type:
Anonymous Authentication
Password Authentication
Individual Certificate Authentication
Signed Certificate Authentication
RADIUS Authentication
NT Domain Authentication
RADIUS or NT Domain Authentication Settings:
Login attempts by password will be verified by the external RADIUS server, Windows NT domain controller, or Active Directory controller.
Specify User Name on Authentication Server
User Name on Authentication Server:
Security Policy
Set Security Policy
Security Policy
Password Authentication Settings:
Password:
Confirm Password:
Individual Certificate Authentication Settings:
The users using 'Individual Certificate Authentication' will be allowed or denied connection depending on whether the SSL client certificate completely matches the certificate that has been set for the user beforehand.
Specify Certificate
View Certificate
Create Certificate
Signed Certificate Authentication Settings:
Verification of whether the client certificate is signed is based on a certificate of a CA trusted by this Virtual Hub.
Limit Common Name (CN) Value
Limit Values of the Certificate Serial Number
Note: Enter hexadecimal values. (Example: 0155ABCDEF)
Hint: Define a user object with username '*' (asterisk) in order to accept a login attempt of a user which does not match any of registered explicit user objects. Such a special user will use the external user-authentication server to verify the login.
OK
Cancel
1 item
1 item selected
Once the required settings are configured, click Close. An advanced management tool for VPN Server / VPN Bridge will be appeared. You can then configure any advanced settings as you wish.
Close
Next >
Close
the setup, you can use the
a Virtual Layer 3 Switch
VPN Server
Site #1
VPN Server / Bridge
Site #3
ENG
12:20 PM
9/21/202

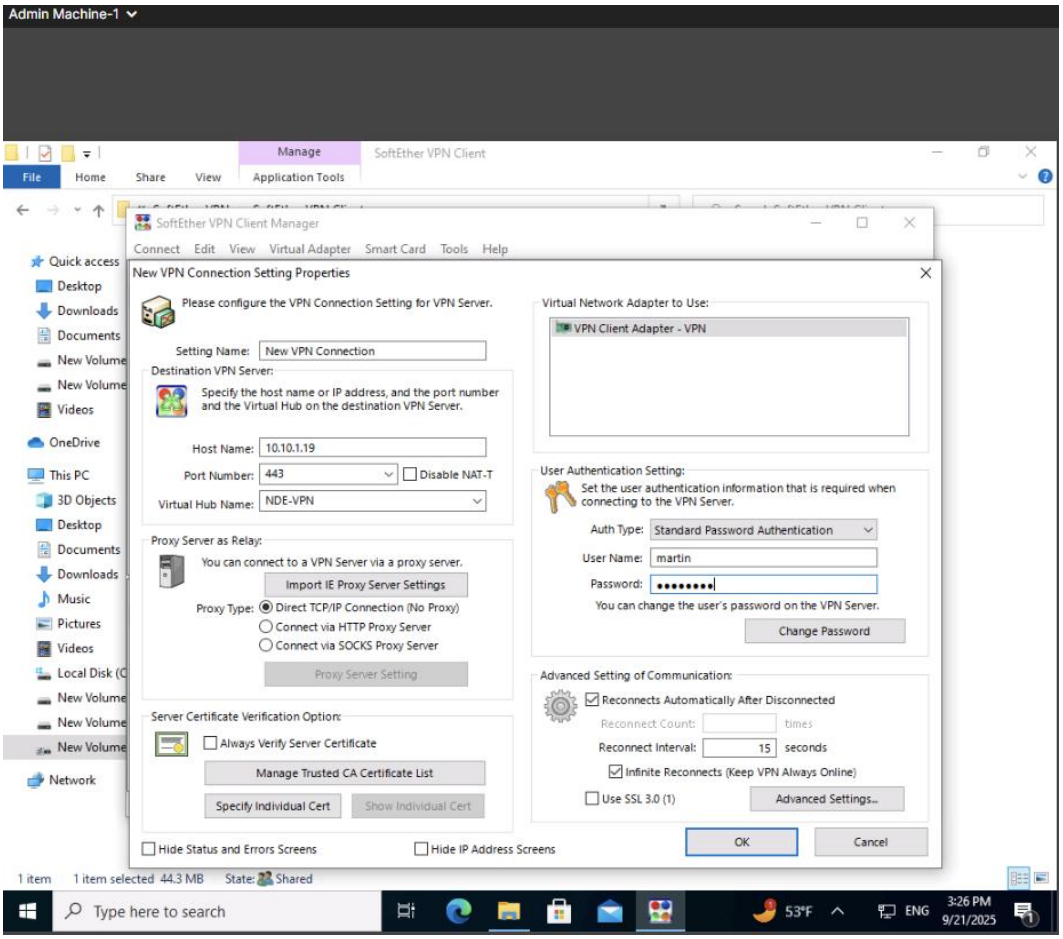

AD Domain Controller
SoftEther VPN Server Manager
localhost (This server) - SoftEther VPN Server Manager
SoftEther VPN Server / Bridge Easy Setup
VPN Easy Setup Tasks
Manage Users
Virtual Hub "NDE-VPN" has the following users.
User Name
Full Name
Group Name
Description
Auth Method
Num Logins
Last Login
martin
martin
-
Password Authe...
0
(None)
New
Edit
View User Info
Remove
Refresh
Exit
Once the required settings are configured, click Close. An advanced management tool for VPN Server / VPN Bridge will be appeared. You can then configure any advanced settings as you wish.
Close
Next >
Close
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
ENG

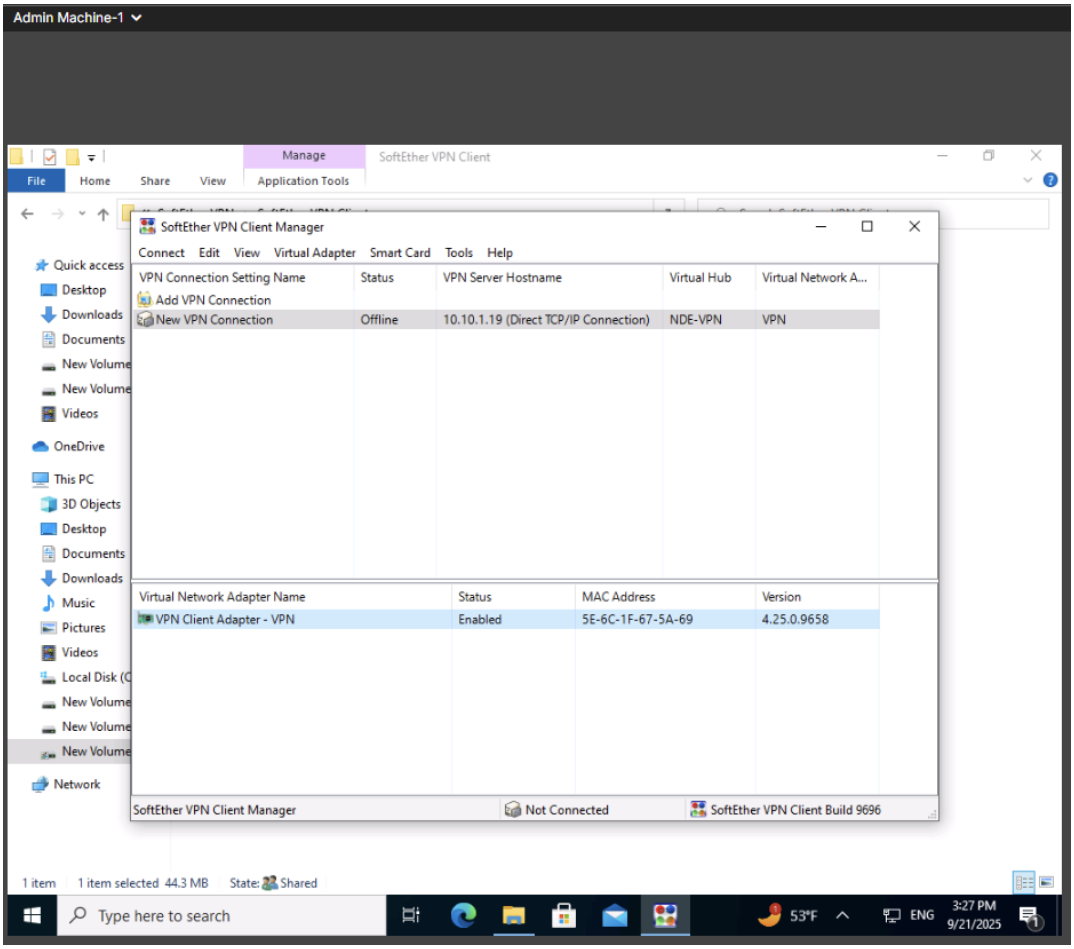

AD Domain Controller
SoftEther VPN Server Manager
localhost (This server) - SoftEther VPN Server Manager
Manage VPN Server "localhost"
Virtual Hub Name
Status
Type
Users
Groups
Sessions
MAC Tables
IP Tables
NDE-VPN
Online
Standalone
1
0
0
0
0
Manage Virtual Hub
Online
Offline
View Status
Create a Virtual Hub
Properties
Delete
Management of Listeners:
Listener List (TCP/IP port):
Port Number
Status
TCP 443
Listening
TCP 992
Listening
TCP 1194
Listening
TCP 5555
Listening
Create
Delete
Start
Stop
VPN Server and Network Information and Settings:
Encryption and Network
Clustering Configuration
View Server Status
Clustering Status
About this VPN Server
Show List of TCP/IP Connections
Edit Config
Local Bridge Setting
Layer 3 Switch Setting
IPsec / L2TP Setting
OpenVPN / MS-SSTP Setting
Dynamic DNS Setting
VPN Azure Setting
VPN Gate Setting
Refresh
Exit
Current DDNS Hostname: vpn776680972.softether.net
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
ENG

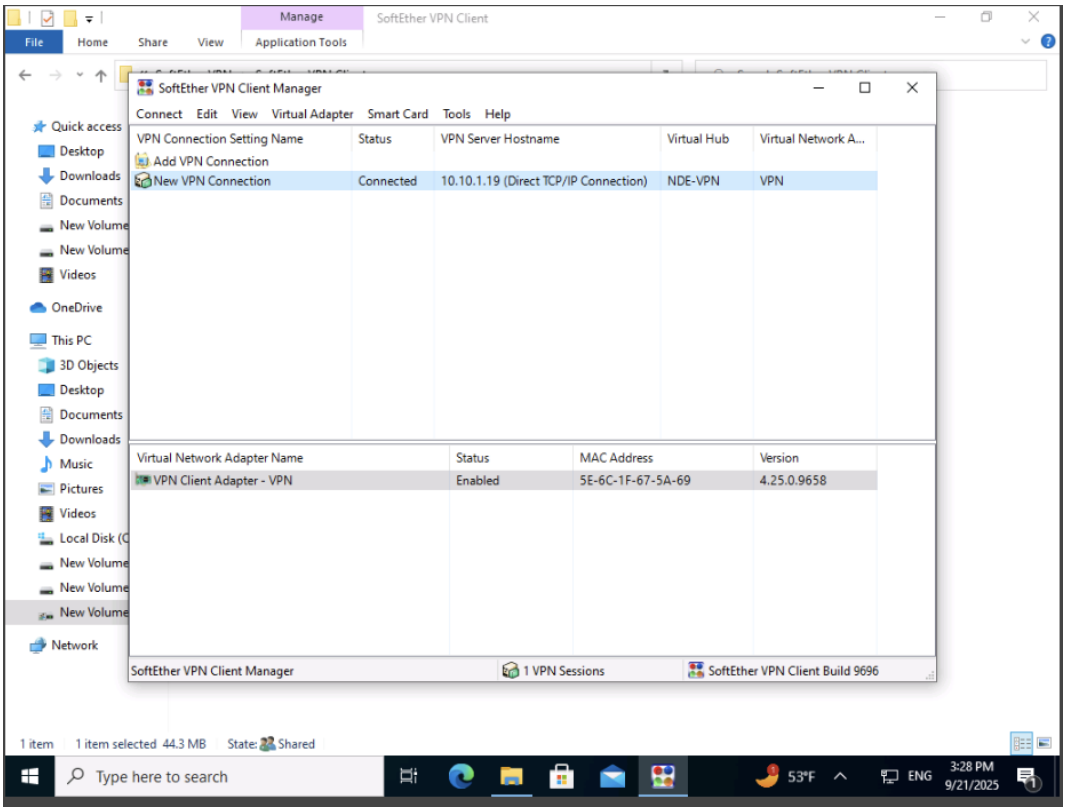

Admin Machine-1
Manage
SoftEther VPN Client
File
Home
Share
View
Application Tools
SoftEther VPN Client Manager
Connect
Edit
View
Virtual Adapter
Smart Card
Tools
Help
VPN Connection Setting Name
Status
VPN Server Hostname
Virtual Hub
Virtual Network A...
Add VPN Connection
Virtual Network Adapter Name
Status
MAC Address
Version
SoftEther VPN Client Manager
Not Connected
SoftEther VPN Client Build 9696
Quick access
Desktop
Downloads
Documents
New Volume
New Volume
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C
New Volume
New Volume
New Volume
Network
1 item
1 item selected 44.3 MB
State: Shared
Type here to search
53°F
ENG
3:24 PM
9/21/2025

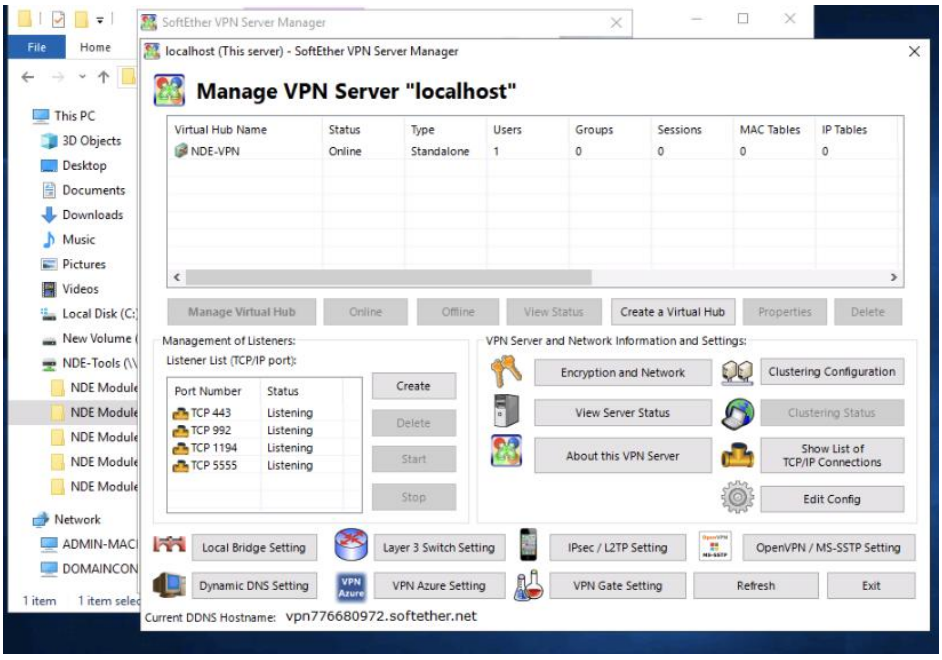

Admin Machine-1
SoftEther VPN Client
File
Home
Share
View
Manage
Application Tools
SoftEther VPN Client Manager (Not Responding)
Connect
Edit
View
Virtual Adapter
Smart Card
Tools
Help
VPN Connection Setting Name
Status
VPN Server Hostname
Virtual Hub
Virtual Network A...
Add VPN Connection
Creating a new Virtual Network Adapter for Windows.
This process can take several seconds or over a minute.
Please wait...
(Please do not perform other operations while the Virtual Network Adapter is being installed.)
SoftEther VPN Client Manager
Not Connected
SoftEther VPN Client Build 9696
1 item
1 item selected 44.3 MB
State: Shared
Type here to search
53°F
ENG
3:25 PM
9/21/2025

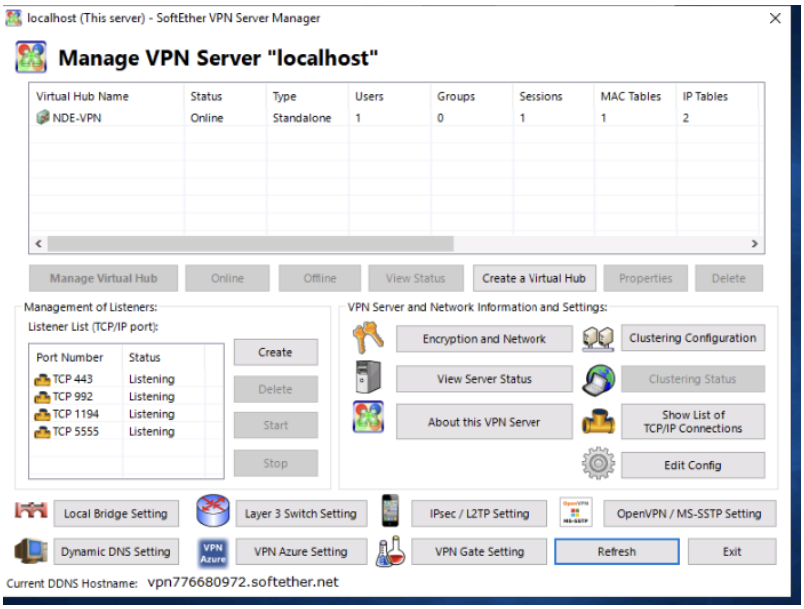

SoftEther VPN Client Manager
Connect
Edit
View
Virtual Adapter
Smart Card
Tools
Help
VPN Connection Setting Name
Status
VPN Server Hostname
Virtual Hub
Virtual Network A...
Add VPN Connection
Virtual Network Adapter Name
Status
MAC Address
Version
VPN Client Adapter - VPN
Enabled
5E-6C-1F-67-5A-69
4.25.0.9658
SoftEther VPN Client Manager
Not Connected
SoftEther VPN Client Build 9696


Admin Machine-1
SoftEther VPN Client
SoftEther VPN Client Manager
Connect Edit View Virtual Adapter Smart Card Tools Help
New VPN Connection Setting Properties
Please configure the VPN Connection Setting for VPN Server.
Setting Name: New VPN Connection
Destination VPN Server:
Specify the host name or IP address, and the port number and the Virtual Hub on the destination VPN Server.
Host Name: 10.10.1.19
Port Number: 443
Disable NAT-T
Virtual Hub Name: NDE-VPN
Proxy Server as Relay:
You can connect to a VPN Server via a proxy server.
Import IE Proxy Server Settings
Proxy Type: Direct TCP/IP Connection (No Proxy)
Connect via HTTP Proxy Server
Connect via SOCKS Proxy Server
Proxy Server Setting
Server Certificate Verification Option:
Always Verify Server Certificate
Manage Trusted CA Certificate List
Specify Individual Cert
Show Individual Cert
Hide Status and Errors Screens
Hide IP Address Screens
Virtual Network Adapter to Use:
VPN Client Adapter - VPN
User Authentication Setting:
Set the user authentication information that is required when connecting to the VPN Server.
Auth Type: Standard Password Authentication
User Name: martin
Password:
You can change the user's password on the VPN Server.
Change Password
Advanced Setting of Communication:
Reconnects Automatically After Disconnected
Reconnect Count: times
Reconnect Interval: 15 seconds
Infinite Reconnects (Keep VPN Always Online)
Use SSL 3.0 (1)
Advanced Settings...
OK
Cancel
1 item 1 item selected 44.3 MB State: Shared
Type here to search
53°F
ENG
3:26 PM
9/21/2025


Admin Machine-1
SoftEther VPN Client
SoftEther VPN Client Manager
Connect Edit View Virtual Adapter Smart Card Tools Help
VPN Connection Setting Name
Status
VPN Server Hostname
Virtual Hub
Virtual Network A...
Add VPN Connection
New VPN Connection
Offline
10.10.1.19 (Direct TCP/IP Connection)
NDE-VPN
VPN
Virtual Network Adapter Name
Status
MAC Address
Version
VPN Client Adapter - VPN
Enabled
5E-6C-1F-67-5A-69
4.25.0.9658
SoftEther VPN Client Manager
Not Connected
SoftEther VPN Client Build 9696
1 item
1 item selected 44.3 MB
State: Shared
Type here to search
53°F
ENG
3:27 PM
9/21/2025


SoftEther VPN Client
SoftEther VPN Client Manager
Connect Edit View Virtual Adapter Smart Card Tools Help
VPN Connection Setting Name | Status | VPN Server Hostname | Virtual Hub | Virtual Network A...
Add VPN Connection
New VPN Connection | Connected | 10.10.1.19 (Direct TCP/IP Connection) | NDE-VPN | VPN
Virtual Network Adapter Name | Status | MAC Address | Version
VPN Client Adapter - VPN | Enabled | 5E-6C-1F-67-5A-69 | 4.25.0.9658
SoftEther VPN Client Manager
1 VPN Sessions
SoftEther VPN Client Build 9696
1 item 1 item selected 44.3 MB State: Shared
Type here to search
53°F
ENG
3:28 PM
9/21/2025


SoftEther VPN Server Manager
localhost (This server) - SoftEther VPN Server Manager
Manage VPN Server "localhost"
Virtual Hub Name | Status | Type | Users | Groups | Sessions | MAC Tables | IP Tables
NDE-VPN | Online | Standalone | 1 | 0 | 0 | 0 | 0
Manage Virtual Hub
Online
Offline
View Status
Create a Virtual Hub
Properties
Delete
Management of Listeners:
Listener List (TCP/IP port):
Port Number | Status
TCP 443 | Listening
TCP 992 | Listening
TCP 1194 | Listening
TCP 5555 | Listening
Create
Delete
Start
Stop
VPN Server and Network Information and Settings:
Encryption and Network
Clustering Configuration
View Server Status
Clustering Status
About this VPN Server
Show List of TCP/IP Connections
Edit Config
Local Bridge Setting
Layer 3 Switch Setting
IPsec / L2TP Setting
OpenVPN / MS-SSTP Setting
Dynamic DNS Setting
VPN Azure Setting
VPN Gate Setting
Refresh
Exit
Current DDNS Hostname: vpn776680972.softether.net



Lab Summary

Exercise 1: Implementing Host-Based Firewall Protection with iptables

Successfully configured firewall rules on an Ubuntu system using iptables. Rules were applied to allow and block specific traffic based on source, destination, and port. This demonstrated basic host-level firewall configuration on Linux.

Exercise 2: Implementing Host-Based Firewall Functionality using Windows Firewall

Configured Windows Firewall to secure an endpoint by adding and enforcing custom inbound and outbound rules. This exercise highlighted how host-based firewalls act as an additional layer of defense in depth by restricting traffic at the system level.

Exercise 3: Implementing Network-Based Firewall Functionality – Blocking Unwanted Website Access using pfSense Firewall

Used pfSense to create aliases and rules that blocked access to unwanted/malicious websites. This exercise showed how aliases simplify firewall management by reducing the number of individual rules required for multiple hosts.

Exercise 4: Implementing Network-Based Firewall Functionality – Blocking Insecure Ports using pfSense Firewall

Configured pfSense to block insecure outbound ports while allowing only trusted services. This reduced exposure to malware and prevented unauthorized outbound communications. Exercise reinforced the distinction between inbound vs outbound firewall rules.

Exercise 5: Implementing Host-Based IDS Functionality using Wazuh HIDS

Initial attempt failed due to a graphical rendering issue in the Security Onion VM, which made the desktop unusable. Restarting the exercise in a new session resolved the problem, and Wazuh HIDS and agent were successfully installed. Network activity was monitored, and alerts were reviewed using Sguil. Demonstrated how HIDS detects anomalous behavior on individual hosts.

Exercise 6: Implementing Network-Based IDS Functionality using Suricata IDS

All installation and configuration steps were completed, including Splunk Enterprise, Npcap, Suricata, and Splunk Forwarder setup. The lab stalled when Suricata failed to start due to a YAML parsing error (Invalid configuration file). The error was not flagged earlier during configuration, which meant over 100 steps were completed before the failure appeared. To finish the exercise, instructor-side screenshots were used to validate expected results (Hydra brute-force attack detection displayed in Splunk).

Exercise 7: Detecting Malicious Network Traffic using HoneyBOT

Configured HoneyBOT as a honeypot to simulate vulnerable services and capture malicious traffic. Observed abnormal traffic patterns that would indicate an attempted attack. This exercise highlighted how honeypots can be used as an early warning system by intentionally attracting malicious actors.

Exercise 8: Establishing Virtual Private Network Connection using SoftEther VPN

Installed and configured SoftEther VPN to establish a secure tunnel. Demonstrated how VPN technology uses HTTPS over TCP/443 to traverse firewalls and NAT devices. Confirmed that a VPN connection can protect communications across untrusted networks.

Reflection

This module covered a wide range of host- and network-based defenses: firewalls, IDS/IPS, honeypots, and VPNs. Most labs were completed successfully, though some encountered issues due to **environment design flaws**:

- **Wazuh HIDS (Exercise 5):** VM rendering glitch required restarting the exercise.
- **Suricata IDS (Exercise 6):** YAML parsing error appeared only at the final execution step, after 100+ tasks. No intermediate error feedback was given, which made troubleshooting especially difficult for a beginner. Instructor screenshots were used to validate expected outcomes.

- The environment imposed a strict **2-hour 15-minute limit for all 8 labs (432 tasks)**, which was unrealistic. To complete the module, each exercise had to be restarted individually to reset the clock.

Despite these limitations, the labs demonstrated how layered defenses work together: firewalls restrict traffic, IDS/IPS detect suspicious activity, honeypots expose attacker behavior, and VPNs secure communications.