IPsec and NAT Support

About IPsec

Internet Protocol security (IPsec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, by using cryptographic security services.

Note You can deploy IPsec in many different ways. This chapter explains what IPsec is and how to secure *selected communication paths* using IPsec. The "IPsec with Network Isolation Utility" chapter explains a more restricted, but automated, application of IPsec to secure the **entire** traffic to and from the server. The Network Isolation Utility also saves you work in applying IPsec. Even if you use this utility to apply IPsec, read this chapter to understand the IPsec deployment options. You can then use the one that is the most beneficial for your environment.

For more information, see https://docs.microsoft.com/en-us/windows/desktop/fwp/ipsec-configuration.

Implementing IPsec in a contact center environment means finding a balance between ease of deployment, usability, and protecting sensitive information from unauthorized access.

Finding the proper balance requires the following:

- Assessing the risk and determining the appropriate level of security for your organization.
- Identifying sensitive information.
- Defining security policies that use your risk management criteria and protect the identified information.
- Determining how the policies can best be implemented within the existing organization.

- Ensuring that management and technology requirements are in place.

How you use or deploy the application influences the security considerations. For example, the required security differs between a single main site deployment and a deployment across multiple sites which might not communicate across trusted networks. The security framework in Windows Server is designed to fulfill stringent security requirements. However, software alone is less effective without careful planning and assessment, effective security guidelines, enforcement, auditing, and sensible security policy design and assignment.

When you enable IPsec, expect negligible impacts on performance with no impact on call processing rates. :

Related Topics

IPsec with Network Isolation Utility

Support for IPsec in Tunnel Mode

Due to increased security concerns in data and voice network deployments, Unified ICM and Unified CCE support IPsec between Central Controller sites and remote peripheral (PG) sites. This secure network implementation implies a distributed model where the WAN connection is secured with IPsec tunnels. The configuration of Cisco IOS IPsec in Tunnel Mode means that only the Cisco IP Routers (IPsec peers) between the two sites are part of the secure channel establishment. All data traffic is encrypted across the WAN link, but unencrypted on the local area networks. Tunnel Mode ensures traffic flow confidentiality between IPsec peers, which are the IOS Routers connecting a central site to a remote site.

The qualified specifications for the IPsec configuration are as follows:

- AES 128
- AES 256

Commonly, QoS networks classify and apply QoS features based on packet header information before traffic is tunnel encapsulated and encrypted.

Support for IPsec in Transport Mode

System Requirements

For IPsec Support in Transport Mode, you need to have Microsoft Windows Server installed.

Supported Communication Paths

Unified ICM Release supports deploying IPsec in a Window Server operating environment to secure server-to-server communication. The support is limited to the following list of nodes, which exchange customer-sensitive data:

1. The connection between the NAM Router and the CICM Router
2. The public connections between the redundant Unified ICM Router/Logger pairs
3. The private connections between the redundant Unified ICM Router/Logger pairs

4. All connections between the Unified ICM Router and the Unified ICM Peripheral Gateway (PG)
5. All connections between the redundant Unified ICM Router/Logger pairs and the Administrator & Data Server (Primary/Secondary) with Historical Data Server (HDS)
6. All connections between the redundant Unified ICM Router/Logger pairs and the Administration Server, Real-time and Historical Data Server, and Detail Data Server (Primary/Secondary)
7. The public and private connections between the redundant Unified ICM PG pair
8. The connections between the redundant Unified ICM PG pair and the Unified Communications Manager in a Unified CCE deployment

For all these server communication paths, consider a *High security* level as a general basis for planning an IPsec deployment.

IPsec Policy Configuration

Windows Server IPsec policy configuration is the translation of security requirements to one or more IPsec policies.

Each IPsec policy consists of one or more IPsec rules. Each IPsec rule consists of the following:

- A selected filter list
- A selected filter action
- Selected authentication methods
- A selected connection type
- A selected tunnel setting

There are multiple ways to configure IPsec policies but the following is the most direct method:

Create a new policy and define the set of rules for the policy, adding filter lists and filter actions as required. With this method, you create an IPsec policy first and then you add and configure rules. Add filter lists (specifying traffic types) and filter actions (specifying how the traffic is treated) during rule creation.

An IPsec Security Policy must be created for each communication path and on each end (on every server). Provide the following when creating and editing the properties of each IPsec policy using the IP Security Policy Wizard.

1. Name
2. Description (optional)
3. Do not Activate the default response rule
4. IP Security Rule (add Rule using the Add Wizard)
    - Tunnel Endpoint (do not specify a tunnel)
    - Network Type: All network connections
5. IP Filter List
    - Name

- Description (optional)
- Add IP Filter using the Add Wizard:

  Description (optional)

  Source address: A specific IP Address (differs based on the path)

  Destination address: A specific IP Address (differs based on the path)

  IP Protocol type: Any
- Add Filter Action using the Add Wizard:

  Name

  Description (optional)

  Filter Action General Options: Negotiate security

  Do not communicate with computers that do not support IPsec

  IP Traffic Security: Integrity and encryption - Integrity algorithm: SHA1 - Encryption algorithm: 3DES
- Authentication Method: Active Directory _Kerberos V5 protocol (Default)

Note

- X.509 certificates can also be used in a production environment depending on customer preference. With Unified ICM requiring Active Directory in all deployment models, relying on Kerberos as the authentication method does not require any extra security credential management. For PG to Unified CM connections, use a pre-shared key (PSK).
- For enhanced security, do not use PSK authentication because it is a relatively weak authentication method. In addition, PSKs are stored in plain text. Only use PSKs for testing. For more information, see the Microsoft Technet articles on pre-shared key authentication.
- If you intend to customize the IPsec policy, you can modify the IPsec setting and customize it. For more information, see the Microsoft Documentation on Configure Data Protection (Quick Mode) Setting.

6. Key Exchange Security Method - IKE Security Algorithms (Defaults)
   - Integrity algorithm: SHA1
   - Encryption algorithm: 3DES
   - Diffie-Hellman group: Medium (DH Group 2, 1024-bit key)

Note

- For enhanced security, use a Diffie-Hellman key of at least 2048-bit strength to mitigate the threat from LogJam vulnerability attacks (CVE - CVE-2015-4000). For more information, see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000. Strong Diffie-Hellman groups combined with longer key lengths increase the computational difficulty of determining a secret key. For more information, see the Microsoft Technet articles on key exchange methods.
- Using longer key lengths results in more CPU processing overhead.

IPsec Connection to Unified Communications Manager

On Unified CCE systems where the Unified Communications Manager is not in the same domain as the Unified ICM system, you cannot use Kerberos for authentication. For such systems, use X.509 certificates.

IPsec Activity

IPsec Monitor

You can use IP Security Monitor (ipsecmon) to monitor IPsec on a Windows Server operating system. For details about the IPsec Monitor, see the Microsoft Technet article.

Enable IPsec Logging

If your policies do not work correctly, you can enable the logging of the IPsec security association process. This log is called an Oakley log. The log is difficult to read, but it can help you track down the location of the failure in the process. The following steps enable IPsec logging.

Procedure

Step 1 Choose **Start** > **Run**.

Step 2 Type **`Regedt32`** and click **OK** to get into the Registry Editor.

Step 3 Double-click **HKEY_LOCAL_MACHINE**.

Step 4 Navigate to `System\CurrentControlSet\Services\PolicyAgent`.

Step 5 Double-click **Policy Agent**.

Step 6 Right-click in the right pane and choose **Edit** > **Add Key**.

Step 7 Enter **Oakley** as the key name (case sensitive).

Step 8 Double-click **Oakley**.

Step 9 Right-click in the left pane and choose **New** > **DWORD Value**.

Step 10 Enter the value name **EnableLogging** (case sensitive).

Step 11 Double-click the value and set the DWORD to **1**.

Step 12 Click **OK**.

Step 13 Go to a command prompt and type **net stop policyagent & net start policyagent**.

Step 14 Find the log in `%windir%\debug\Oakley.log`.

Message Analyzer

Message Analyzer enables you to capture, display, and analyze protocol messaging traffic; and to trace and assess system events and other messages from Windows components.

For more information on Message Analyzer, see Microsoft Documentation.

System Monitoring

The built-in Performance console (perfmon) enables you to monitor network activity along with the other system performance data. Treat network components as another set of hardware resources to observe as part of your usual performance-monitoring routine.

Network activity can influence the performance not only of your network components but also of your system as a whole. Be sure to monitor other resources along with network activity, such as disk, memory, and processor activity. System Monitor enables you to track network and system activity using a single tool. Use the following counters as part of your usual monitoring configuration:

- Cache\Data Map Hits %
- Cache\Fast Reads/sec
- Cache\Lazy Write Pages/sec
- Logical Disk\% Disk Space
- Memory\Available Bytes
- Memory\Nonpaged Pool Allocs
- Memory\Nonpaged Pool Bytes
- Memory\Paged Pool Allocs
- Memory\Paged Pool Bytes
- Processor(_Total)\% Processor Time
- System\Context Switches/sec
- System\Processor Queue Length
- Processor(_Total)\Interrupts/sec

NAT Support

Network Address Translation (NAT) is a mechanism for conserving registered IP addresses in large networks and simplifying IP addressing management tasks. NAT translates IP addresses within private *internal* networks to *legal* IP addresses for transport over public *external* networks (such as the Internet). NAT also translates the incoming traffic *legal* delivery addresses to the IP addresses within the inside network.

You can deploy IP Phones in a Unified CCE environment across NAT. You can locate remote Peripheral (PG) servers on a NAT network remote from the Central Controller servers (Routers and Loggers). NAT support qualification for PG servers was limited to a network infrastructure implementing Cisco IP Routers with NAT functionality.

Agent Desktops are supported in a NAT environment, except when silent monitoring is used. Silent Monitoring is not supported under NAT.

For more detailed resources on how to configure NAT, see https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml.

For more details on how to deploy IP Phones across NAT, see https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/12-4t/nat-12-4t-book.pdf.

IPsec and NAT Transparency

The IPsec NAT Transparency feature introduces support for IPsec traffic to travel through NAT or Port Address Translation (PAT) points in the network by addressing many known incompatibilities between NAT and IPsec. VPN devices automatically detect NAT Traversal (NAT-T). If both VPN devices are NAT-T capable, then NAT-T is autodetected and autonegotiated.

Other IPsec References

- IPsec Architecture: https://technet.microsoft.com/en-us/library/bb726946.aspx
- See Microsoft documentation for details on Windows Server.
- Windows Firewall and IPsec: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security